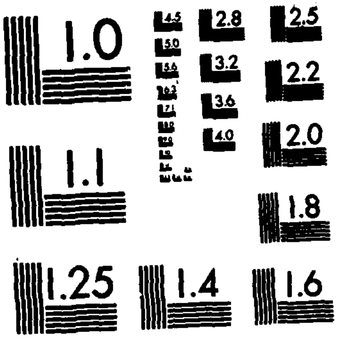
AD-A126 167 ANALYTICAL PROCEDURES FOR TESTABILITY(U) OKLAHOMA UNIV 1/4
NORMAN SCHOOL OF INDUSTRIAL ENGINEERING A A ALY ET AL.
JAN 83 RADC-TR-83-4 F30602-81-C-0012

UNCLASSIFIED F/G 14/2 NL


1.0
4.5
5.0
5.6
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

(12)

RADC-TR-83-4
Final Technical Report
January 1983

ANALYTICAL PROCEDURES FOR TESTABILITY

University of Oklahoma

Adel A. Aly and Jon C. Bredeson

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

ROME AIR DEVELOPMENT CENTER
Air Force Systems Command
Griffiss Air Force Base, NY 13441

This report has been reviewed by the RADC Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RADC-TR-83-4 has been reviewed and is approved for publication.

APPROVED: Jerome Klion

JEROME KLION
Project Engineer

APPROVED: Rudolf R Konegen

RUDOLF R. KONEGEN, Major, USAF
Assistant Chief
Reliability & Compatibility Division

FOR THE COMMANDER: John P. Huss

JOHN P. HUSS
Acting Chief, Plans Office

If your address has changed or if you wish to be removed from the RADC mailing list, or if the addressee is no longer employed by your organization, please notify RADC (RBET) Griffiss AFB NY 13441. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document requires that it be returned.

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER RADC-TR-83-4	2. GOVT ACCESSION NO. AD-A126 167	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) ANALYTICAL PROCEDURES FOR TESTABILITY		5. TYPE OF REPORT & PERIOD COVERED Final Technical Report Nov 80 - Apr 82
		6. PERFORMING ORG. REPORT NUMBER N/A
7. AUTHOR(s) Adel A. Aly Jon G. Bredeson		8. CONTRACT OR GRANT NUMBER(s) F30602-81-C-0012
9. PERFORMING ORGANIZATION NAME AND ADDRESS University of Oklahoma School of Industrial Engineering Norman OK 73019		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 62702F 23380251
11. CONTROLLING OFFICE NAME AND ADDRESS Rome Air Development Center (RBET) Griffiss AFB NY 13441		12. REPORT DATE January 1983
		13. NUMBER OF PAGES 294
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) Same		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report) Same		
18. SUPPLEMENTARY NOTES RADC Project Engineer: Jerome Klion (RBET)		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Fault Detection, Fault Isolation, Testability, Diagnostics, Test Systems, Maintainability		

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The objective of this study was to develop an analytical base of methodologies and procedures to be used in the testability area. Testability is a subset of systems maintainability and is defined by the system fault detection and isolation capability. During this effort a comprehensive survey of the open and closed literature was performed to determine the analytical concepts, models, algorithms and definitions which are presently in use in the testability area. The findings were summarized, analyzed and evaluated. The results contained in the report include a comprehensive listing, definition, and discussion of commonly used testability parameters and their components; discussion of the problems, and critiques, of certain of the commonly used parameters; a summary discussion of all analytical testability models, analyses techniques and algorithms which were found to exist in the literature; an appendix which contains full summaries of all the survey material; recommendation for modifications of existing procedures and for future research are also made.

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. Introduction

1.1 Background

The problem of fault isolation techniques has not advanced noticeably during the last two decades. The basic process that existed was manual signal tracing. This process relied heavily on the technical expertise of the maintenance technician. Even with highly skilled personnel this process was slow and difficult since it required a large array of test equipment such as signal generators, oscilloscopes and voltmeters as well as extensive technical manuals. As a consequence many faults were not correctly diagnosed; the extensive use of trial and error substitution as a means of identifying the faulty part created problems; time required to perform fault isolation was large and as a consequence system availability was low.

The next (and current) era came with its technological advances in electronics, the transistor, integrated circuit, small, medium and large scale integration and better packaging techniques. These allowed the practical development of ever increasingly complex systems and necessitated the development of a modular diagnostic concept. At that point in time, automation was introduced into the fault isolation process at the system, subsystem and equipment levels. The fact of the matter is, however, that advances in electronic technology have overpaced the technology of efficient and effective fault isolation design. Few new procedures or techniques have been developed to aid in the design of cost effective automated fault isolation systems and as a result current automation is complex, costly and has been seen to be ineffective in a large percentage of applications. Therefore, the problem of diagnosis is shifted from locating the faulty discrete component to the identification of the line replaceable unit (LRU) in which the faulty component is resident. An LRU may include smaller modules within it to facilitate offline replacement or it can itself be the lowest level of replacement.

The introduction of digital computers and microprocessors as part of the system provide an automatic testing procedure. Basically, the design of built-in-test (BIT) diagnostic subsystems along with the selection of test points where the test equipment are attached will provide an efficient, less expensive, and more reliable fault isolation procedure.

A selfdiagnosability is recognized when the organizational BIT will automatically execute a primary sequence of diagnostic tests to identify malfunctioning subsystems up to a given group of LRUs. As faults are localized, malfunctioning groups of LRUs can be replaced (by switching on standby spares) and a secondary isolation may be performed by external organizational tests (semi-automatically) or by shop and depot tests (automatic or manual) to isolate the single failed unit or component.

1.2 Related Research

A review of the technical literature yields a surprising small number of references to the general problem of efficient or optimum diagnostic procedures. The references which do exist appear to be related to the definition of efficient and optimum means for choosing a given set of diagnostic tests necessary to isolate a given fault. One of the earliest models proposed for relating faults to diagnostic tests is that of Brulé et al. (1960).* In this model, the system is represented as an interconnected collection of functional elements with access to the terminals of the available elements. Tests are performed on collections of elements; hence the test-fault relationship is a test-element relationship and a fault is considered to be the failure of an element in performing its function. A related work by Johnson (1960) discusses the generation of efficient sequential test procedures by use of information theoretic methods to evaluate the amount of information provided by a test. Chang (1965) develops a different criterion for evaluating the "goodness" of the available tests. He introduces the distingishability criterion for a set of n singly occuring faults, where m tests are considered for inclusion in a fixed test schedule. The model is a data matrix D having entry d_{ij} = 1 if test T_j fails for fault f_i, and d_{ij} = 0 if test T_j passes for fault f_i. Distinguishability among the rows of the table is considered and the model is applied to the selection of a fixed set of diagnostic tests. Butterworth (1972), Firstman and Gluss (1960) develop search procedures to determine a sequence which minimizes the expected cost of secondary isolation to locate a failed element within a group of LRUs identified by the BIT primary diagnostic. Cohn and Ott (1971) present an optimal algorithm to minimize the expected cost of the test tree. The test tree specifies an adaptive testing procedure that detects a

*The paper and/or report pertaining to this work and others referenced in this section is summarized in the appendix of the report.

failure and isolates the faulty component. They utilize a recursive formula for their optimal search. Even though they recognize the similarity to the machine setup problem and the applicability of dynamic programming techniques to solve the problem, their adaptive procedure is exactly a dynamic programming procedure. Sheskin (1978) develops a probabilistic dynamic programming procedure to determine the sequence of diagnostic tests to isolate the group of modules which contains the faulty unit.

From the above survey, only Cohn and Ott and Sheskin solve the sequencing problem optimally by utilizing dynamic programming. Unfortunately, no computational experiences are presented. If dynamic programming is used, and the number of elements in the equipment increases, the computational and storage burden increases exponentially. Therefore, their approach is not practical in solving a real testability problem.

Aly (1979) presents a Branch-and-Bound algorithm to solve the problem of optimum design diagnostics (fault detection and isolation). Although no computational experience is provided the algorithm has a great tendency to reduce both the computation and storage burden in comparison to the above ones. Aly (1980) develops several dominance and reduction rules which improve the performance of the algorithm developed previously. Aly and Elsayedaly (1981) provide comprehensive computational results for the branch-and-bound algorithm and also show its superiority over other methods developed based on dynamic programming.

In the literature very few studies address the problem of the composite test systems, taking into account combinations of organization built-in-test, external organizational test, shop test, and depot test. Several do however, treat various components of the problem. Bogard et al. (1980) develop several cost estimating relationships to estimate the operation and support costs associated with various types of BIT and external test equipment (TE). These estimates are developed through application of engineering cost estimating and regression analysis techniques. Consolla and Danner (1980) and Pliska et al. (1979) present various figures of merit to measure the effectiveness of BIT/TE. Tuttle and Loveless (1980) present the BIT/TE reliability impact on prime equipment design and maintenance downtime using correlation analysis.

None of the references which were found address the optimization of the entire composite system. Also, as will be seen in the sections which follow, some of the figures of merit are inconsistent to be effective in the design of the prime systems.

1.3 Task Makeup of the Overall Effort

A description of the tasks which make up the overall effort and a summary discussion of why each task was undertaken follows.

1.3.1 Baseline Definition

The first task is the definition of a baseline of tools and methodologies related to the optimal design of fault detection and isolation procedures. The list of possible baseline tools will include but will not necessarily be limited to:

i. Acquisition, operation, and support cost:
Operation and support costs are increasing more rapidly than acquisition cost. This results from the need for and cost of support equipment, skilled operators and maintenance personnel to handle the current complex and sophisticated equipment and systems in use today. The use of BIT and TE may reduce these costs. However, too much automation may not be cost effective, and trade-offs to achieve the optimum combination are required.

ii. Reliability, maintainability, and availability:
The reliability of the system when BIT/TE is used will depend on the BIT/TE capability, size and the thoroughness (time and accuracy) of both detection and isolation capabilities. Besides the reliability of BIT/TE, the reliability of the primary system depends on the frequency of failure of each LRU, the criticality of failures, and the effects of failure.

iii. Testability trade-offs:
The trade-offs include the different testability attributes of the composite systems. The main factors impacted are in the economic and availability/maintainability/reliability realms.

1.3.2 Mathematical Models Assessment

The primary goal of this task is to determine the factors that affect the choice and development of models. This will help in assessing the effectiveness of fault detection and isolation for both single test systems and for composite test systems. Existing or developed models will be evaluated for each of the possible applications by posing such questions as:

- Is this type of model appropriate to the testability function?
- Are all the important phenomena and tools included?
- Is the level of detail commensurate with the answers sought?

Based on experiences and from the comprehensive literature survey no hybrid model exists to date to logically and quantitatively measure testability effectiveness.

1.3.3 Literature Review of Other Fields

From a review of the available literature (see Appendix) it was discovered that there are several other fields which developed and utilized techniques analogous to the ones used in electronic system diagnostics. In chemical engineering Himmelblau (1978) discussed the use of fault detection and isolation techniques in chemical plants. Chemical plants today are characterized by complex processes and equipment which lead to a high cost of downtime. Thus, the detection and analysis of faults in process equipment are of definite economic significance in both the design and operation of a plant. In the area of medical diagnosis "A Sequential Approach to Heart-Beat Internal Classification" applies sequential testing to a Markovian model of cardiac rhythm intervals. An on-line implementation of a sequential classification procedure in a coronary care ward is evaluated. In the toxicology field "A System of Computer Aided Diagnosis with Blood Serum Chemistry Tests and Bayesian Statistics" utilizes computer aided diagnosis tests to detect the type of poison in the blood. In computer science, there are enormous amounts of paper dealing with fault detection and isolation in logical and digital systems, for instance see Carroll and Smith (1972).

This research effort will include the following:

i. Identification and collection of reports published in the open literature which describe methods and techniques applicable to testability. For those techniques which are judged and selected to be of an advanced or unique nature, the operating and data requirements will be identified.

ii. To the extent possible, the identification and description of fault detection and isolation techniques in use by industry and government agencies in other fields (nonelectronic).

1.3.4 Analysis of New Existing Techniques

Based on the needs of this effort, the adequacy of the available methods will be assessed, and limitations identified. Potential areas for research modifications are those areas with properties similar to testability and/or where the correct techniques are most apparent. Effort will be made to structure the research effort to coincide with the defined baseline.

1.3.5 Evaluation of Models and Techniques

The research effort will include the evaluation of new and updated models and techniques in terms of the data required by each for their implementation. This task involves the evaluation of each model in terms of its form and makeup as well as the availability and cost of physically reliable data needed to drive the technique to a logical and optimal solution. However, no attempt to mechanize the methodologies or algorithms will be made.

1.4 Report Organization

This report is organized to provide insight into the basic analytical tools to be utilized in the area of testability. The effectiveness of testability parameters and variables will be explored and mathematically analyzed to provide an evaluation for each measure considered. In most of the report a heavy emphasis is towards the models and parameters obtained from the literature.

The remainder of the report is organized into four sections and one major appendix. Section 2 addresses the testability parameters and their makeup. An Engineering discussion of BIT/TE use and characterization is presented. BIT/TE use at various levels of maintenance and their impacts on various characteristics of the system is discussed. Section 3 deals with the problems and critiques of the testability parameters. Section 4 treats all testability models, analysis procedures and algorithms which were found to exist in the literature. Basically, it is separated between current testability technology and technology from related areas directly applicable to testability.

The Appendix contains the full summaries of all the surveyed materials. Each publication is analyzed to cover the following: Title, Author, Journal, Scope, Problem definition, Assumptions, Solution approach, Computational experience, and Conclusions. A general classification is designed to furnish a framework for all research under different criteria.

2. TESTABILITY PARAMETERS - THEIR MAKE-UP AND RATIONALE

The purpose of this section is two-fold:

a. To describe the composition and nature of currently used testability parameters, rationale and implementation means.

b. To provide an insight into these variables which impact the testability parameters, testability rationale and implementation means. The latter, in particular, will serve to provide visibility relative to the complexities and the factors involved in testability evaluation, analysis and optimization.

Current testability theory was found to revolve around the following assumptions. The primary equipment is composed of modular line replaceable units (LRUs). Whenever the equipment malfunctions, a single LRU is assumed to have failed, and two types of diagnostic tests may be used for primary and secondary isolation. The primary isolation tests will be automatically executed by the Built-in-Test (BIT) in order to identify the LRU or group of LRUs which contains the faulty unit. After the execution of the automatic BIT, secondary isolation if required will be performed by semiautomatic, external test equipment (TE) or manual means to locate the single failed unit within a group of LRUs.

After an LRU (or LRUs) is removed from the equipment it is brought to an intermediate shop location where isolation to the failed subunit of the LRU is performed. This isolation is performed either by intermediate shop test equipment by manual means or a combination of both. A hot mockup for LRU failure verification and checkout may or may not be used.

Accuracy or failure of BIT or of an external tester, while not directly affecting prime equipment operation, can adversely impact system availability and contribute to logistic problems. Hence the reliability and efficiency attributes of external testers and BIT affect system reliability and life-cycle cost to a significant degree.

The following subsections have several purposes:

a. To introduce in a simple fashion testability, components, the basic logic of testability, the commonly used parameters and the terms associated with testability.

b. To provide a feel for the different variables which must be considered in making evaluations, developing models, performing design and cost optimizations, and trade-offs.

2.1 Integrated Built-In-Test

BIT diagnostic subsystems are incorporated in electronic equipment to minimize downtime in the event of a failure, and because they allow for fewer and less qualified maintenance personnel and fewer pieces of external test equipment.

BIT subsystems can perform three basic functions. They can be used as a system monitor, they can be used to test for system readiness prior to and during operation, and to isolate a fault in order to facilitate repair.

2.1.1 Built-In-Test Variables

Many characteristics and variables must be considered in designing the BIT system because of their effect on the final testability and cost of the system and the role they play in the BIT and external test trade-off. They include:

a. Failure modes and effects which are distinguishable and traceable.

b. Size and weight of BIT hardware.

c. Maintenance constraints levied on the system.
   i. Time limitations for fault isolation.
   ii. Maintenance manhours per flying hour.

d. Size and function of the LRUs.
   i. The relative frequency of failure of each LRU.
   ii. The criticality of failures.
   iii. The number of LRUs to which the BIT system initially isolates.

e. Average maintenance manhours required for manual troubleshooting to isolate to an LRU in the event the BIT system does not recognize a failure has occurred.

f. Average maintenance manhours per BIT system preventive maintenance action (provided PM is applicable to BIT system).

g. Average failure rate of BIT (based on components of BIT not needed for prime equipment function).

h. Average failure rate of prime equipment(s) which BIT serves (does not include failure rate of parts belonging uniquely to BIT), in failures/flying hours.

i. Service life.

j. Average cost/BIT failure (material, spares, etc.).

k. Average manhours required to repair a BIT failure.

l. Proportions of prime equipment faults detectable and not detectable by BIT.

m. Cost/maintenance manhour.

n. Average cost to determine failure which has occurred in two cases:
   i. If the incidence of failure is evident even though BIT is incapable of detecting it.
   ii. Failure may remain undetected until primary system mission commitment and so cause mission abort or failure.

o. False alarm rate.

2.1.2 Effectiveness of the BIT

The basic effectiveness of BIT diagnostic subsystems depends on the *following:*

a. The percentage of system "faults" which cannot be verified at the organizational level which were BIT discovered (can not duplicate, false alarms).

b. The percentage(s) of actual system faults detected and/or isolated by BIT and simple visual examination at the organizational level of maintenance.

c. The average number of removals per failure.

2.1.3 BIT Circuitry "Failure Modes and Types"

The four major "failure modes" caused by BIT circuitry are:

a. Induced failures
   - BIT causes failure of prime equipment.

b. False alarm
   - BIT reports a failure of the prime equipment when none exists.

c. Failure to report

- BIT does not indicate a failure when system has a valid failure (a failure of the type that BIT was designed to indicate).

d. False report
- BIT incorrectly identifies a nonfailed unit.

2.2 External Testers

External test equipment (TE) (of different types) is used in organizational, intermediate, or depot maintenance levels to isolate failures and verify LRU or Shop Replaceable Unit (SRU) repair results. The use of test equipment during the repair cycle to isolate faults to the desired logistic elements affects total reliability and life cycle cost to a significant degree. External testers are usually used at higher levels of the maintenance chain to isolate to the faulty subunit (for example a failed printed circuit board contained in a LRU). They can, however, be used at lower levels to augment BIT or be used in lieu of BIT. The choice of the extent of use of TE at any level is contingent on costs, mission characteristics, and requirements.

The decision to perform external testing through use of ad hoc testers or by other means depends on the maintenance policies which are possible and/or the alternatives available for troubleshooting/diagnosis. Examples of such policies/alternatives are:

a. Whether or not it is possible for isolation to be done by randomly removing or replacing the LRUs (after they have been isolated to a group by BIT or after their arrival at the intermediate shop). In this case the availability of means for testing the replaced LRUs (either by checking out the system at organizational level or by having available a hot mockup at the intermediate level) has to be considered as well as the material, manpower, and time resources that would be required.

b. Whether or not a sequential troubleshooting guide is available.

2.2.1 External Testing Variables

Characteristics and variables that must be considered in the selection or design of external tester concepts and hardware.

a. The hardware level at which the external tester is to be used (i.e., a printed circuit board tester)

b. Its volume and weight constraints

c. Portability characteristics

d. Its software costs, hardware costs

e. Maintenance constraints levied
   i. Time limitations for isolation
   ii. Maintenance manhours per maintenance action

f. Utilization rate

g. Proportion of faults in a given LRU isolatable by tester

h. Maintenance costs of the testers (scheduled and unscheduled maintenance)

i. Failure rate of the tester

j. Service life

k. False alarm rate

l. Its function (use at organizational maintenance level to augment or take place of BIT, use at intermediate level to test and isolate faults in LRUs)

m. Manpower or manhour costs associated with applications to system fault isolation

2.2.2 Effectiveness of External Test Subsystems

The basic effectiveness of external test subsystems depends on the following:

a. The percentage of units which "test as failed" by the test system, but which, on subsequent test at other maintenance levels, test as "operational".

b. The percentage of unit faults (LRU or SRU) (assuming the external test subsystem is to be used for the isolation of such faults) that can be isolated by the external tester.

c. The time and manpower costs associated with test subsystem application.

2.3 Diagnostic System Parameters

The following parameters can be considered in any BIT/TE system:

2.3.1 Fraction of Faults Detected (FFD)

The Fraction of Faults Detected (FFD) is defined in the literature in several ways:

a. the fraction of all faults detected (or detectable) by BIT/TE (FFD_A).

$$FFD_A = \frac{\text{quantity of faults detected by BIT/TE } (Q_{BDF})}{\text{quantity of all faults } (Q_F)}$$

b. the fraction of all detectable faults detected (or detectable) with BIT/TE (FFD_D).

$$FFD_D = \frac{\text{quantity of faults detected by BIT/TE } (Q_{BDF})}{\text{quantity of faults detected } (Q_{FD})}$$

c. the fraction of all faults detected, through use of defined means (FFD_V).

$$FFD_V = \frac{\text{quantity of faults detected, through use of defined means } (Q_{VDF})}{\text{quantity of all faults } (Q_F)}$$

"Defined means" implies all means of detection which have been identified, documented, defined.

Example:

a. Visual Means

b. BIT/TE Means

c. Semiautomatic Means

d. Manual Means

It is important to notice that

a. "Detected faults" is used synonymously with "detectable faults".

b. Intermittent faults must be classified as a single fault.

c. Temporary faults are not faults, and so must be excluded from Q_F, Q_{FD}, Q_{VDF}, and Q_{BDF}.

d. There are significant but subtle differences among these.

Q_F, Q_{FD}, Q_{BDF} and Q_{VDF} may be defined either as faults which may be observed while the system is in operation (or may be determined by weighting each possible fault by its frequency of occurrence over a hypothetical period of operating time) or as the absolute number of faults possible without taking frequency of failure (failure rate) into account.

FFD is useful in describing the coverage of the built-in-tests, and it correlates with the objective of measuring "fault detection accuracy" and "thoroughness", but as can be seen it is subject to various interpretations.

2.3.2 Fraction of False Alarms (FFA)

False Alarms are those indications of a fault when an actual fault has not occurred. The Fraction of False Alarms may be defined in various ways.

FFA_A is the fraction of all BIT/TE indicated faults which are false alarms.

$$FFA_A = \frac{\text{quantity of BIT/TE false alarms } (Q_{FA})}{\text{quantity of all BIT/TE indicated faults } (Q_{BIF})}$$

FFA_B is the ratio of the quantity of BIT/TE false alarms to the quantity of faults detected through use of defined means.

$$FFA_B = \frac{\text{quantity of BIT/TE false alarms } (Q_{FA})}{\text{quantity of faults detected through use of defined means } (Q_{VDF})}$$

FFA_C is the ratio of false alarms to actual faults (or the ratio of false alarm rate to failure rate).

$$FFA_C = \frac{\text{quantity of BIT/TE false alarms } (Q_{FA})}{\text{quantity of all faults } (Q_F)}$$

Again note, the significant, but very subtle differences among the above three definitions.

If BIT/TE is an integral part of the system, a false alarm occurs only when the BIT/TE and the system are operational but BIT/TE indicates a fault.

The most common causes of False Alarms are:

a. Faulty BIT/TE function

b. Out-of-tolerance conditions of BIT/TE components

c. Transient conditions (not true faults) occurring during operation in a planned stable environment

Fault indications which are not false alarms, but which are sometimes mistaken as such could be:

a. Intermittent failures

b. Transients or performance changes occurring in the prime system as a consequence of environmental variation

2.3.3 Fraction of False Status or Isolation Indications (FFSI or FFII)

The Fraction of False Status Indications is the fraction of BIT/TE fault indications (or lack thereof) which are erroneous.

$$\text{FFSI} = \frac{\text{quantity of false alarms and undetected faults}}{\text{quantity of BIT/TE indicated faults and undetected faults}}$$

If BIT is considered to be an integral part of the system then undetected faults occur when an operational BIT fails to detect a fault or when BIT is not operational (no matter what the equipment status is).

If BIT is considered to be independent of the system then undetected faults occur when an operational BIT fails to detect a fault or when BIT and the system are both not operational.

FFSI correlates with the objective of measuring "fault detection accuracy".

The Fraction of False Isolation Indications is the fraction of BIT or TE isolations that identify the wrong removable unit (subunit) or group of units (subunits) as failed.

$$\text{FFII} = \frac{\text{quantity of failures for which BIT/TE erroneously diagnoses the wrong unit or group of units as failed}}{\text{quantity of actual failures for which BIT/TE identified a unit or group of units as failed}}$$

FFII and FFSI are primarily indicators of design problems resulting either from test system design error, low sensitivity thresholds or tolerance levels of system/equipment components and signals. They can create serious consequences by causing confusion during fault detection and isolation and by eroding maintenance technician confidence in the test system.

2.3.4 Mean Fault Detection Time (T_{FD})

The Mean Fault Detection Time is the average time it takes for BIT to detect and indicate a fault from the time the fault has occurred. T_{FD} may also be defined as the time to indicate a fault or to detect a fault once it has occurred.

It can be interpreted in a variety of ways.

T_{FD_A} is the average time to detect and indicate a fault.

$$T_{FD_A} = \frac{\sum_{i=1}^{Q_F} \text{(time to detect and indicate the } i^{th} \text{ fault)}}{\text{quantity of faults } (Q_F)}$$

T_{FD_B} is the average time to detect and indicate a BIT/TE detectable fault.

$$T_{FD_B} = \frac{\sum_{i=1}^{Q_{BDF}} \text{(time to detect and indicate the } i^{th} \text{ BIT/TE detectable fault)}}{\text{quantity of faults detected by BIT/TE } (Q_{BDF})}$$

T_{FD} correlates with the objective of measuring "fault detection time".

2.3.5 Mean BIT/TE Running Time (T_B)

T_{FD_j} is the average time to detect and indicate a fault through means j.

$$T_{FD_j} = \sum_{i \varepsilon j} \frac{\text{(time to detect and indicate the } i^{th} \text{ fault belonging to means } j)}{\text{quantity of faults belonging to detection means } j}$$

The Mean BIT Running Time is the average active time to perform a BIT test routine. This can be the average for one test, a group of tests, or all tests.

T_B will generally be limited to fault detection where the tests are periodic, continuous or timeshared, and serial (nonoverlapping). The cases considered in the average will be both with and without a fault being found. The tests may be such that testing stops when a fault is found or such that the testing routine continues to completion.

When T_B is low we can expect the Mean Fault Detection Time (T_{FD}) to be low also.

$$T_B = \frac{\sum_{i=1}^{N_B} \text{(active running time of the } i^{th} \text{ BIT/TE test routine, } T_{B_i}\text{)}}{\text{the number of BIT/TE test routines } (N_B)}$$

2.3.6 Frequency of BIT/TE Executions (F_B)

The Frequency of BIT Executions is the cycling rate at which periodic BIT tests are executed. This does not apply to BIT tests that are executed only upon request. F_B^{-1} = the time to execute the complete set of BIT tests plus the idle time between executions.

A cycle is defined as the time from the start of a given BIT test until the same test is started again. For cases where all tests do not have the same periodicity the cycle time is considered to be the largest cycle time of all the BIT tests.

2.3.7 Test Thoroughness (TT)

Test Thoroughness is the fraction of the equipment (system) tested by BIT/TE relative to the entire equipment (system). Some possible parameters of measure are the failure rate, the number of functions, the number of components and the number of faults tested and untested.

Note that TT will equal the Fraction of Faults Detected (FFD) if the same parameter of measure and the same level of measure (e.g. component level) are used.

A high TT implies that most components, functions, etc. are tested, and correspondingly a low number of undetected failures result. Thus a high TT is desirable and if not achieved for the TT of BIT alone should be achieved for the TT of BIT and external testers combined.

$$TT = \frac{\text{amount of system/equipment tested by BIT/TE}}{\begin{array}{l}\text{amount of system/equipment} \\ \text{tested by BIT/TE}\end{array} + \begin{array}{l}\text{amount of system/equipment not} \\ \text{tested by BIT/TE}\end{array}}$$

2.3.8 Fraction of Faults Isolated (FFI)

The Fraction of Faults Isolated (FFI) may be interpreted and applied in a number of different ways.

The Fraction of Faults Isolated (FFI_A) is the fraction of those faults detected by BIT/TE which are then isolated with BIT to the ıeplacement level as defined by the maintenance concept.

$$FFI_A = \frac{\text{quantity of detected faults isolated with BIT/TE } (Q_{IB})}{\text{quantity of faults detected } (Q_{FD})}$$

The Fraction of Faults Isolated (FFI_B) is the fraction of all faults capable of being isolated by BIT, defined semiautomatic, and/or manual means or a combination of these. (It includes all faults, detectable or not).

$$FFI_B = \frac{\text{quantity of faults isolated by defined means}}{\text{quantity of faults occurring}}$$

The Fraction of Faults Isolated FFI_c (FFI_d) (FFI_e) - is the fraction of all faults capable of being isolated by BIT, (by semiautomatic means), (by manual means).

$$FFI_i = \frac{\text{quantity of faults isolated by i means}}{\text{quantity of faults occurring}}$$

$i = c, d, e$

All of the above have subtle but significantly different interpretations. All have impact on system/equipment design and cost.

2.3.9 Fault Isolation Resolution (FIR(L))

Fault Isolation Resolution may be interpreted and applied in a number of different ways.

The Fault Isolation Resolution ($FIR(L)_A$) is the fraction of detected faults isolated by BIT to an acceptable (specified) maximum number of replaceable items.

$$FIR(L)_A = \frac{\text{quantity of detected faults isolatable to} \leq \text{L LRUs by BIT/TE}}{\text{quantity of detected faults}}$$

The Fault Isolation Resolution ($FIR(L)_B$) is the fraction of all faults capable of being isolated by any or all defined means (BIT, semiautomatic, external test, manual) to an acceptable (specific) maximum number of replaceable items.

$$FIR(L)_B = \frac{\text{quantity of faults isolated to} \leq \text{L LRUs}}{\text{quantity of faults}}$$

The Fault Isolation Resolution ($FIR(L)_B$), can refer to faults isolated by semiautomatic means, external test, manual means or by all combination of such means.

Both of the above have subtle but significantly different interpretations. All have significant impact on system/equipment design and cost.

FIR(L) is usually specified for more than one value of L.

A high FIR(L) is typically the result of extensive BIT capability. This capability results in a high degree of BIT/TE fault isolation and thus a low Fault Isolation Time (T_{FI}) is expected. This high degree of BIT fault isolation would also result in a lower Maintenance Personnel Skill Level (MPSL).

2.3.10 Mean Fault Isolation Time (T_{FI})

The Mean Fault Isolation Time is the average time to complete the fault isolation process.

A low T_{FI} is typically the result of extensive BIT capability which also results in a high Fraction of Faults Detected (FFD), a high Fraction of Faults Isolated (FFI), and a low Maintenance Personnel Skill Level (MPSL) requirement.

T_{FI} can be interpreted in a variety of ways.

As T_{FI_A} is the average time to complete the fault isolation process using BIT/TE,

$$T_{FI_A} = \frac{\sum_{i=1}^{Q_{BDF}} \text{(time to isolate the } i^{th} \text{ fault with BIT/TE)}}{\text{quantity of faults detected } (Q_{FD})} .$$

As T_{FI_B} is the average time to complete the fault isolation process taking into account all defined means,

$$T_{FI_B} = \sum_{i=1}^{Q_F} \frac{\text{(time to isolate the } i^{th} \text{ fault)}}{\text{quantity of faults } (Q_F)} .$$

As T_{FI_j} is the average time to complete the fault isolation process through means j (BIT/TE, semiautomatic, manual, etc.)

$$T_{FI_j} = \sum_{i \epsilon j} \frac{\text{(time to isolate the } i^{th} \text{ fault belonging to } j)}{\text{quantity of faults belonging to } j} .$$

All of the above have subtle but significantly different interpretations. All have significant impact on system/equipment design/cost.

2.3.11 Maintenance Personnel Skill Level (MPSL)

The Maintenance Personnel Skill Level is either (a) the average skill level required or (b) the minimum skill level required to perform corrective maintenance for a system/equipment. All maintenance actions must be capable of being performed by a specified quantity of maintenance personnel with a specified skill level, at various maintenance levels. BIT must be designed for use by a specified minimum skill level technician.

2.3.12 BIT/TE Reliability ($MTBF_{B/E}$)

BIT/TE Reliability is the probability that the BIT/TE circuitry will perform its intended function for a specified interval under specified conditions. BIT circuitry is any hardware that is used for BIT testing that is not common to the system hardware.

$$MTBF_{B/E} = \{\lambda_{B/E}\}^{-1} = \{\sum_{k=1}^{N_{B/E}} \lambda_{B/E_k}\}^{-1}$$

where $N_{B/E}$ = quantity of BIT/TE hardware components not common to the system hardware

λ_{B/E_k} = failure rate of the kth BIT/TE hardware component.

2.3.13 BIT/TE Maintainability ($MTTR_{B/E}$)

BIT/TE Maintainability is the average time to repair a fault in the BIT/TE hardware.

$$MTTR_{B/E} = \frac{\sum_{k=1}^{N_{B/E}} \lambda_{B/E_k} \quad M_{CT_k}}{\sum_{k=1}^{N_{B/E}} \lambda_{B/E_k}}$$

where M_{CT_k} = repair time for the kth BIT/TE hardware component.

2.3.14 System Maintainability - Mean Time To Repair (MTTR)

System Maintainability or Mean Time to Repair is the average corrective maintenance time for all system/equipment faults. MTTR is the elapsed time from start of work on the correction of a malfunction indication to the completion of the maintenance action and verification of the correction.

$$MTTR = \frac{\sum_{i=1}^{N} \lambda_i \quad M_{CT_i}}{\sum_{i=1}^{N} \lambda_i}$$

where N = number of system hardware components

λ_i = failure rate of the ith hardware component

M_{CT_i} = repair time for the ith hardware component.

M_{CT_i} is a function of Fraction of Faults Detected, Fraction of Faults Isolated, Mean Fault Detection Time, Fault Isolation Resolution, and Mean Fault Isolation Time, as well as set-up time, remove/repair/replacement time, checkout time. One simple model for M_{CT_i} may be represented as follows:

(Assuming fault resolution level of 1)

$$*M_{CT_i} = (FFD_1)(T_{FD1})+(FFD_2)(T_{FD2})+(FFI_1)(T_{FI1})+(FFI_2)(T_{FI2})+T_{SU}+T_{RR}+T_{CU}$$

More complex models can be constructed which take into account Resolution Levels, Fraction of False Status or Isolation Indications, or Fraction of False Pulls.

where

FFD_1 = fraction of faults detected by some defined means

FFD_2 = fraction of faults not detectable by a defined means

T_{FD1} = mean fault detection time of faults belonging to FFD_1

T_{FD2} = mean fault detection/recognition time of faults belonging to FFD_2

FFI_1 = fraction of faults isolated by some defined means

FFI_2 = fraction of faults not isolated by some defined means

T_{FI1} = mean fault isolation time of faults belonging to FFI_1

T_{FI2} = mean fault isolation time of faults belonging to FFI_2

T_{SU} = mean setup time

$*T_{RR}$ = mean remove/replace/repair time

T_{CU} = mean checkout time

*as indicated, this is a rather simple representation.

MTTR is a measure of the adequacy of the system in meeting real operational requirements. One must first determine the critical operational requirements which may be sortie generation rate for aircraft, missile build-up/generation rate, etc. This requirement then becomes the driving function for the value MTTR can assume and still enable all mission scenarios to be accomplished.

2.3.15 BIT/TE Availability ($A_{B/E}$)

BIT/TE Availability is a measure of the degree to which the BIT/TE circuitry is in the operable and committable state at the start of a mission, when the mission is called for at an unknown (random) point in time.

$$A_{B/E} = \frac{MTBF_{B/E}}{MTBF_{B/E} + MTTR_{B/E}}$$

2.3.16 System Availability (A)

System Availability is a measure of the degree to which the system/equipment is in the operable and committable state at the start of a mission, when the mission is called for at an unknown (random) point in time.

$$A = \frac{MTBF}{MTBF + MTTR}$$

In order to get an appreciation of the impact of testability attributes on availability, reference is made to 2.3.14 where MTTR is broken down into its testability parameters.

2.3.17 Fraction of False Pulls (FFP)

The Fraction of False Pulls is the fraction of LRUs removed from a system, due to the result of the BIT/TE fault detection/isolation process that are good LRUs (i.e. LRUs with no actual fault).

$$FFP = \frac{\text{quantity of good LRUs removed } (Q_{GLR})}{\text{quantity of LRUs removed } (Q_{LR})}$$

FFP is partially maintenance concept dependent. It depends on the number of LRUs to which the fault is isolated. For example Fault Isolation Resolution (FIR(L)).

If x is the average fault isolation group size then for replacement of the entire group of LRUs, $FFP = \frac{x-1}{x}$; and for iterative LRU replacement done randomly, $FFP = \frac{\frac{(x+1)}{2} - 1}{\frac{(x+1)}{2}} = \frac{x-1}{x+1}$. This can be derived from FIR(L) given the replacement concept to be used. It is also dependent on the number of False Alarms experienced during the period and the Fraction of False Status or Isolation Indications.

Oftentimes the definition of this term is used to define/specify only one or more of its contributing parameters. Unless this is specifically defined, confusion and ambiguity are present.

2.3.18 Fraction of Erroneous Fault Isolation Results (FEFI)

The Fraction of Erroneous Fault Isolation Results is the fraction of BIT/TE fault isolation results that identify the wrong LRU once a fault has been detected. FEFI measures how well the BIT fault isolation function has been documented in maintenance manuals and software. FEFI can be interpreted in a number of ways.

$$\mathrm{FEFI}_A = \frac{\text{quantity of erroneous fault isolation results } (Q_{EFIR})}{\text{quantity of fault isolation results } (Q_{FIR})}$$

$$\mathrm{FEFI}_B = \frac{\text{quantity of erroneous fault isolation results } (Q_{EFIR})}{\text{quantity of faults } (Q_F)}$$

Again we see subtle but significant differences in the interpretation of the parameter.

2.3.19 Can Not Duplicate (CND)

When the BIT diagnostic routine indicates a system fault resulting in a write-up and subsequent trials of the test or subsequent troubleshooting at the organizational level of maintenance reveals no fault indications, the corrective action is coded as a CND.

A CND can be caused by factors such as test tolerances too tight or not applicable to the domain of the failure mode, momentary excursions from the measured test parameter, effects of other equipment loading factors, test voids, testing incompatibilities, operator error, maintenance error, false alarms, technical order error, and the inability during troubleshooting to duplicate conditions of flight dynamics (g forces, temperature, vibration, etc.). For example, an intermittent failure may be caused during normal system operation by environmental stresses such as temperature or vibration. Such stresses are rarely present in the maintenance environment.

Whatever their cause, CND events result in the expenditure of resources without valid system repair. Labor is expended investigating faults which do not exist, which is most significant during surge conditions. CND maintenance actions lower the confidence of the technician in the diagnostic capability of BIT and distort the evaluation of FD/FI capability.

2.3.20 Retest Okay (RTOK)

A RTOK is a malfunction which, when detected and isolated by the automatic diagnostics at one level of maintenance, is not detectable at a higher level.

For aircraft systems, many malfunctions occur in integrated systems, wirings, mechanical solenoids, and electrical relays and connections which were never intended to be addressed by the automatic FD/FI systems. These malfunctions may induce incorrect FD/FI indications of avionics malfunctions. This situation results in extensive manual troubleshooting and high RTOK rates at intermediate and depot levels of maintenance.

There are numerous other possible causes of RTOK events. One possibility is that the lower level diagnostic system was in error and identified the wrong unit as the cause of the malfunction.

Another possible cause that has received more attention in recent years in a lack of vertical testability. Ideally, as a unit moves from one level of maintenance to the next higher level, the unit should be subjected to increasingly stringent test parameters. However, what has recently been seen is that test tolerances at the higher levels may be the same or less stringent than the tolerances of lower levels. Much of this can be attributed to the equipment being developed under different contracts with unrelated system specifications.

A high percentage of RTOK events means that assets are being put into the repair cycle that may not be faulty, or that may not get fixed. This denies the use of apparently serviceable assets for the period of the repair cycle, reduces the confidence of the technicians in the diagnostic programs, and degrades the practical FD/FI capability of the BIT/TE.

Methods for reducing the impact of repair cycle times are:

a. increase the reliability of equipment units to decrease the frequency of their entry into the repair cycle.

b. develop intermediate level test capabilities to allow verification of a failed unit before submitting it to the repair cycle.

c. increase the spares level of certain SRUs to compensate for units in the repair cycle.

d. give high priority to the expeditious repair and distribution of equipment critical components.

2.3.21 Percent of Maintenance Over 3 Hours (EMT_3)

In studying the reported charged maintenance time for use in evaluating BIT, an effectiveness criteria is required. The criteria should be related to BIT's purpose of low maintenance times. The measurement which best meets this is the percentage of maintenance actions exceeding a fixed time. Based on data, Tuttle and Loveless (1980) choose an over-3-hour (EMT_3) value as a criteria for excessive maintenance time.

2.3.22 Not Ready for Issue (NON-RFI)

The percent of units issued which fail functional checks when installed.

2.3.23 Percent BIT

The percent of the unit which is made up of BIT, as quantified by failure rates.

2.3.24 Percent Tested

The percent of the unit which is tested by BIT, as quantified by failure rates. This is sometimes used synonymously as FFD_A or FFI_A. However, "tested" is ambiguous as it is unclear whether it refers to detection, isolation or both.

2.3.25 Percent TE Failures

Test equipment failures as a percentage of prime equipment failures. Here ambiguity is introduced by the word "failures". It is unclear if it pertains to actual TE component failures or includes such things as design errors which cause false alarms, misassignments or failure to be able to be used as planned.

2.3.26 Known False Alarm (KFA)

A Known False Alarm is a failure reported erroneously by BIT because of anomalies in the diagnostic software. Conditions known to cause BIT false alarms are identified as KFAs in the handbooks and manuals along with their failure codes. In some cases, KFAs constitute a large percentage of all BIT failure reports. The chief impact of KFAs on BIT effectiveness is a reduction in technician confidence.

2.3.27 Test Aborts

A test abort occurs when a test is initiated and automatically stops before completion. This is reported to the technician as a failure, but the report is coupled to a stop code. Test aborts are generally indicative of software deficiencies.

2.3.28 Percentage of Addressable Faults Correctly Detected

Where addressable faults are defined as those faults which BIT is designed to detect.

2.3.29 Percentage of Addressable Faults Correctly Isolated

Where addressable faults are defined as those faults which BIT is designed to detect/isolate.

2.3.30 Percentage of Time Correct Fault Isolation Achieved by the FD/FI System While Operating in the Automatic Mode

2.3.31 System MTTR (in Clock Hours/Maintenance Action)

a. for automatic mode FD/FI operation

b. for manual mode FD/FI operation

2.3.32 Percentage of Maintenance Actions Accomplished Using Automatic FD/FI Procedures When Compared to the Total Number of Maintenance Actions

2.3.33 Percentage of Maintenance Actions Accomplished Using Manual (Beyond FD/FI) Procedures

2.3.34 Maintenance Man-Hours (MMH)/Maintenance Action (MA)

The maintenance man-hours per maintenance action are the total maintenance man-hours (MMH) charged for the period divided by the number of maintenance actions charged to a unit. The crew size and off-line support contribute to the MMH.

MMH/MA is a function of Fraction of Faults Detected, Fraction of Faults Isolated, Mean Fault Detection Time, Fault Isolation Resolution, Mean Fault Isolation Time, as well as other factors.

2.3.35 Maintenance Man-Hours (MMH)/Operating Hour (OH)

Similar to the above except that the total maintenance man-hours for the period is divided by the total operating hours of the unit during that period.

2.4 Built-In-Test External Test Trade-Offs

The trade-offs between BIT and external/semiautomatic/manual test systems can be decided taking into account the values of the proportions of equipment failures identifiable and isolatable by the equipment's BIT (e.g., 95% of all equipment faults shall be detectable by the equipment's BIT capability) and external/semiautomatic/manual test systems consistent with the requirements on mean time to repair and maintenance manhours. This shall be accomplished by modelling the maintenance manhours or mean time to repair which results from each mix, comparing this with the requirements and estimating the acquisition support and manpower costs associated with each mix.

The trade-offs between these two diagnostics depends also on the maximum number of LRUs which can comprise a group of LRUs, isolatea by a given set of diagnostics, the average proportion of faults in each LRU or group of LRUs detectable by each diagnostic, and reliability characteristics of each LRU.

2.5 Level of Repair (LOR)

In general level of repair can be classified according to where the repair is to be done (maintenance level), and the size of the units being tested and isolated (hardware levels).

2.5.1 Maintenance Level

a. **Organizational Level**
The first level (lower level) of repair usually at the site of the equipment (on the airplane, at the radar station, etc.)

b. **Intermediate Level**
The second level of repair, in the maintenance shop

c. **Depot Level**
The highest level of repair, in the main depot

2.5.2 Hardware Levels

a. **Line Replaceable Units (LRUs)**
LRUs are the largest components to be isolated. At the organizational level it could be a single LRU or a group of LRUs. They are typically the "black boxes".

b. **Shop Replaceable Units (SRUs)**
SRUs are components of the LRUs (cards). The faulty SRUs are identified and replaced at the intermediate level of maintenance.

c. **Piece Parts**
Piece parts are the smallest components of the SRUs.

2.6 The Maintenance Scenario

The prime consideration in any maintenance plan is repair at the organizational level and keeping minimum traffic in the repair and/or logistics pipeline with special emphasis upon personnel, training and spares.

Combining the maintenance and hardware levels, a general maintenance plan consists of replacement of LRUs (one or more) at the organizational level. At the intermediate level, the LRUs are tested using shop testers (external tests) and the faulty modules (SRUs) are isolated and replaced. Some of these SRUs are forwarded to the depot level for eventual more specialized repair.

At the organizational level, time is the single most important factor. Every effort should be made to reduce the mean time to repair (MTTR), or otherwise to increase availability. The group of LRUs (or a single LRU) which contains the faulty unit is isolated after executing the automatic BIT and/or other detection/ isolation means. With the advent of BIT the trend has been to reduce the number of special purpose external testers at organizational levels. Little or no effort is taken to replace the SRUs within the LRUs at this level. This is done at the ıntermediate level. An SRU is usually replaced at the organization level only in cases of emergency such as exhausted spares (LRUs in this case).

After isolating the group of LRUs which most likely contains the faulty unit, three possibilities arise:

a. Send the group of LRUs to the shop (intermediate level) for further examination in order to isolate the faulty LRU and SRU.

b. Send the LRUs defined as faulty directly to the depot after some rudimentary tests are performed to attempt to isolate the operational LRUs from the faulty.

c. Throw portions of the group of LRUs away (after defined tests are performed to isolate the faulty LRUs), if it will not be worth repairing or the cost of introducing it into the maintenance cycle and the incurred cost of labor and time for its repair is not economical (will cost more than the original cost of these LRUs).

For each one of the previous possibilities, there is a chance that the isolated group of LRUs does not contain the faulty unit. That results from either a false report from the BIT (False Status or Isolation Indication, or a False Alarm) without having any malfunction whatsoever. The decision of where to handle the isolated group of LRUs is not an easy one. It will depend on many factors related mainly to the nature of LRUs themselves and the performance of the BIT at the organizational level, the costs involved at this level, and the cost consequences of any decision made for the organizational level on the higher levels of maintenance. Factors which play a role in making this decision are:

a. number of LRUs which constitute the isolated group of LRUs by BIT

b. whether or not semiautomatic tests / manual tests on the group are possible/permissible such that further intragroup isolation can be achieved.

c. size of the LRUs and their cost

d. number of SRUs in each LRU

e. types and modes of failure of the SRUs

f. size of the SRUs and their cost

g. proportion of false alarms of the BIT/TE system

h. proportion of false reports of the BIT/TE system

i. proportion of faults detected by the BIT/TE system

j. proportion of RTOKs

At the higher levels (intermediate and depot), more specialized work can be done because of the availability of sophisticated equipment as well as skilled labor besides relatively ample time to do the testing.

At the intermediate level, the group of LRUs isolated by the BIT at the organizational level will be examined for LRU verification and faulty SRU isolation.

This can take place in a number of ways:

a. A hot mockup can be utilized to verify which of the LRUs are faulty.

b. Each LRU can be tested on a specialized piece of test equipment (perhaps a portion of the tester capable of troubleshooting the LRU down to its faulty SRUs).

The decision to send the LRUs to an intermediate level of maintenance impacts prime system readiness or availability, spares requirements, costs for support and test equipment and manpower requirements and costs. At the intermediate level, after testing the LRUs and isolating the defined faulty SRUs two possibilities present themselves:

a. Send the defined faulty SRUs to the depot for test. This implies shipping and handling charges on top of depot costs relating to manpower, material, and specialized and general test equipment. It also impacts turnaround time and logistics considerations.

b. Discard the SRU. This impacts logistics considerations as far as the need for purchases and supplies of new SRUs over the lifetime of the system.

Both possibilities will be affected with respect to the quantity of CNDs associated with the LRUs tested. No matter which course of action is chosen, if the intermediate level of maintenance concept is implemented, costs of the manpower and test equipment (both special purpose and general) and their characteristics (i.e., faulty SRU detection, isolation, false isolations, etc.) must be taken into consideration.

In the instance where the LRUs defined as faulty (at the organizational level) are sent directly to depot, two alternatives must be considered:

a. Send all LRUs in the group isolated, to depot. This would incur minimum manpower and support equipment costs at the base (site level) but would increase logistics needs at the LRU level and shipping and handling costs. The depot would incur increased manpower costs, CND rate would increase and more and different types of test equipment would have to be installed at the depot.

b. Perform rudimentary tests on the LRU, perhaps on a hot mockup or a GO, NO GO tester and send only these LRUs defined as faulty to the depot. This would incur some increased degree of manpower and support equipment costs at the base (site level) and would also impact logistics needs at the LRU level (but, to a lesser extent than the previous alternatives). The depot would incur increased manpower costs (but to a lesser extent than the previous alternative), CND rate would increase and more and different types of test equipment (but fewer types than with the previous alternative) would have to be installed at the depot.

In the instance where the LRUs are discarded at failure, the result is no costs for manpower and support equipment at the higher maintenance level. A much larger and continuing logistics burden at the LRU level will however result. The burden will be increased by false alarms, high levels of resolution, false indications.

Since the cost and manpower requirements for each of the three possibilities are impacted by the components of the LRUs as well as the accuracy of the testing, the maintenance concept must be determined based on the characteristics of the individual system under consideration.

3. PROBLEMS AND CRITIQUES OF TESTABILITY PARAMETERS

In the previous sections, as was noted for various parameters, there **exist subtle** but significant differences in interpretation. But even accepting these differences, ambiguities in interpretation due to semantics and lack of clarity in definition still persist. Take for example the three definitions for **Fraction of Faults Detected** (FFD). In particular consider the terms: Q_{BDF} (Quantity of faults detected by BIT/TE), Q_{FD} (Quantity of faults detected) and Q_{VDF} (Quantity of faults detected through use of defined means). Q_{BDF}, Q_{VDF} and Q_{FD} have in some instances been calculated taking into account both false alarms and false indications. In at least as many cases the terms have been calculated taking into account only **detections caused by actual faults** (failures). In only rare cases are the terms defined such that no confusion exists. (Semantics used play a key role in the confusion. For example, the phrase "quantity of faults detected" is not synonymous with the similar phrase "quantity of fault detections" yet examples of their use have been seen).

Taking into account the three interpretations of FFD and the two possible interpretations of a term or quantity which appears in each, we are left with six possible interpretations of FFD. But wait, we may not have as yet exhausted all possible ambiguities. When we define Q_{BDF}, Q_{FD}, and Q_{VDF} do we mean all possible faults or the faults which will occur over a period of system operating life (in accord with failure rates). Taking these two possibilities into account we are left with 12 possible interpretations of FFD.

The impact of the considerations of failure rate in testability parameters merits further discussion. Whether or not failure rate is considered in defining testability requirements and during testability design, it is **always** considered during testability evaluation and measurement. Take for example FFD_A, where **quantity of faults** is a variable in both numerator and denominator. If data on such quantities are collected for a given system or equipment over time (which is invariably the case) then the value of FFD_A calculated will be a function of the **relative values of the failure rates** of the units making up the equipment/system.

Cases have been found where equipment and systems have been designed for FFD defining that parameter as the fraction of all (possible) faults detectable, rather than the fraction of all faults detectable (over any given period of operating time) and evaluated using the latter definitions. In other words, FFD was designed for (and perhaps specified) using one definition and evaluated using a second.

The Fraction of Faults Isolated (FFI) parameter has problems of exactly the same type and we are left hereto with 12 possible interpretations. In addition, the same problems have been found to exist with respect to semantic imprecision and to the consideration of failure rates.

Fault Isolation Resolution (FIR(L)) has similar ambiguities. Again does or does not Q_{FD} (quantity of detected faults) include false alarms or false status indications? Is or is not failure rate taken into account in defining quantity of faults (failures)? The result is eight different possible interpretations.

Fraction of False Status or Isolation Indications (FFSI) or (FFII) also have ambiguities inherent to their definition and use, for example with respect to treatment of failure rates.

In summary, the same nature of comments can be made for many of the most commonly used testability parameters. In general, the problem with all of the above can be traced to inadequate and ambigious definition of terms, parameters and their meanings. In many instances for example a system requirement might state a Fraction of Faults Detectable (or Fraction of Faults Isolatable) of 90% and no more information. As discussed previously, there are 12 different interpretations possible for each requirement (parameter). Clearly associated with each parameter must be unambiguous data which defines under which ground rules, and assumptions, the parameter applies.

Other problems exist as well. Classifying intermittent faults as a single fault ignores its effects on the many Can Not Duplicates (CNDs) and Retest Okays (RTOKs) which can occur as a consequence of the single fault. Both consequences should be considered or the effects of intermittent faults should be taken care of in some other unique manner. The same argument may be applied as to whether or not false alarms should be classified as corrective maintenance actions, BIT detections, or not included in such categories at all.

As seen, there are many testability parameters, some dependent and some apparently independent of others, which exist. The existence of many different parameters leads to problems in system optimization (or even overall testability evaluation). For this reason, it would seem to be desirable to be able to logically group two or more testability parameters into a single meaningful parameter. Several attempts at this have been attempted. All have been less than entirely valid from a mathematical/ engineering standpoint.

For example, even though different parameters are used to determine both the accuracy of fault detection and fault isolation, many automatic fault detection/ fault isolation systems (which use built in test (BIT) capability to detect and identify malfunctions and use a fault isolation test capability to isolate the detected malfunction to some specific level in the system) use only one figure, FD/FI, as an indication of the diagnostic system capability. For example 90%/80% means 90% of those malfunctions addressable by the FD/FI capability are detected and of those detected 80% are isolated. Since the percentage of faults detected and isolated are considered independent it can be concluded that 72% of the addressable malfunctions can be isolated.

Actually this figure is misleading since it provides no real insight as to the true system capability. This is quite obvious from looking at the definition and the meaning of the FD/FI figure, where the following deficiencies can be observed:

a. The FD/FI figure disregards the unaddressable malfunctions (all malfunctions which are not covered by the fault detection system).

b. It disregards the undetected faults (because the fault detection is not 100%). Therefore all addressable faults which are undetected are neglected.

c. It ignores the possibility that fault detection is not necessarily independent of fault isolation. A fault which is easy (difficult) (impossible) to detect, due to its nature is oftentimes, for the same reasons, easy (difficult) (impossible) to isolate. This will affect the validity of the joint figure.

d. It is ambigous with respect to how false alarms, false detections, false pulls or false isolations are to be interpreted.

Each of the above factors will affect the percentage of fault detection and percentage of fault isolation as well as the FD/FI figure. Consequently, the actual diagnostic system capability may differ from any conclusion based on the FD/FI figure; and in order to make this figure of any significant or practical meaning, the above factors, namely dependence, independence, false alarms, and resulting CNDs and RTOKs should be considered in a more thorough methodology to evaluate FD/FI systems. Accurate evaluation of the FD/FI capability must encompass a determination of how many maintenance actions are addressable by the FD/FI system, how many of those are actually solved using the automatic mode, how many resort to the manual mode (for which well defined procedures exist), how many required manual solutions for which there are no established procedures, how many were nonaddressable malfunctions, how many malfunctions resulted in maintenance actions which could not find the malfunction (CND) and how many maintenance actions fell into special categories.

Also, it is observed that the BIT/TE parameters are defined and determined as if the levels of maintenance have nothing to do with them and their values, which is not true since test tolerances are different at different levels, they are supposed to be tighter at the intermediate level than at the organization level, and they are supposed to be tighter at the depot level than at the intermediate level. This criterion by itself needs more investigation. However, its effects on the FD/FI can not be neglected and should be included. There might be a way to represent the FD/FI parameters such that knowing how tight the test tolerance is, a figure can be used to determine the FD/FI of the system, an idea similar to the concept of computing an estimate of a population mean within a certain level of confidence in statistics.

Earlier we discussed the ambiguities associated with the definition of FFD and FFI parameters. The following relates to another serious problem relating to these same parameters, namely the analytical means through which such parameters may be analytically evaluated during the design process. It deals with the observation that the majority of methods used to calculate the fault detection coverage of self-test programs, designed to test digital circuits, make the assumption that the probability of occurrence of all solid faults in the digital circuits is equally likely. As a result of this assumption, the percent fault detection coverage found by using these methods cannot take into account different probabilities of occurrences of faults. If some of the undetected faults in the system are more likely to occur than the faults which are detected, then the percent fault detection capability of the self-test program is overestimated. If, on the other hand, the undetected faults have very low probabilities of existence, then the derived fault detection capability value for the self-test program is not an overestimate. Therefore, the question is: How can the probability of occurrences of fault affect the percent fault detection coverage?

3.1 MATHEMATICAL APPROACH

From the above discussion, it is seen that in order for any BIT/TE parameter to be reliable enough to be used in determining the accuracy of the FD/FI system more rigorous investigation and analysis are required.

In this section an example of such an analysis is explained for the last case concerning the probability of occurrences of faults. Definitions and mathematical formulas which make use of the statistically weighted parameters to better define BIT/TE parameters are presented.

The analysis includes a procedure for combining the results of a method used to find the percent structural fault detection coverage of a self-test program with the results of a method used to calculate the probability of occurrences of all faults considered in the analysis. The methods are combined to calculate a statistically weighted percent fault detection coverage. A number of the BIT/TE parameters are defined as ratios of quantitites. Some of these are Fraction of Faults Detected (FFD), Fraction of False Alarms (FFA), Fraction of False Status Indications (FFSI), etc. These ratios are only appropriate when faults have equal probability of occurrence. If not, these fractions or ratios can give misleading indications.

3.2 ASSUMPTIONS

a. A digital circuit node fails due to either a stuck at zero or a stuck at one fault.

b. Only one node can fail in the circuit at any given time (a reasonable assumption after the circuit has been initially tested).

c. The probability of a stuck at one or stuck at zero fault is not the same.

3.3 DEFINITIONS

The word "fault" indicates a stuck at zero or stuck at one fault at a circuit node. Whereas "an error" indicates a symptom or indication of a failure at a test point which may normally be an output.

Definition 1. A circuit node which carries no undetected faults at any test point (output) is a detected node.

Definition 2. An undetected node is a circuit node which carries an undetected stuck at zero, stuck at one, or both at any test point (output).

Let

n = total number of nodes in the circuit

m = number of test points (outputs) in the circuit

Let x_i represent the ith node in the circuit where $i = 1, 2, \ldots\ldots n$. Let y_j represent the jth test point (output) in the circuit, where $j = 1, 2, \ldots\ldots m$. Define two random variables X_i and Y_j such that

$$X_i = \begin{cases} 0\text{--stuck at zero fault on node } x_i \\ 1\text{--stuck at one fault on node } x_i \\ 2\text{--fault free node } x_i \end{cases}$$

$$Y_j = \begin{cases} 0\text{--test point (output) node } y_j \text{ fault free} \\ 1\text{--test point (output) node } y_j \text{ has an error} \end{cases}$$

The $P(X_i = 0, X_j = 0) = 0$ because only one node can fail at any given time. The probability of a stuck at zero fault at a node x_i occurring and being detected is

$$P\ X_i = 0 \cap (Y_1 = 1 \cup Y_2 = 1 \cup \ldots . \cup Y_m = 1)$$

This is equivalent to the probability that the stuck at zero fault occurs on node x_i and at least one of the test points (output) nodes is in error. Now

$$P\ X_i=0 \cap (Y_1=1 \cup Y_2=1 \cup \ldots \cup Y_m=1) \quad = P\ (Y_1=1 \cup Y_2=1 \cup \ldots \cup Y_m=1) | X_i=0\ P\ X_i=0$$

The $P\ (Y_1=1 \cup Y_2=1 \cup \ldots \cup Y_m=1) | X_i=0 = 1$ if the stuck at zero fault on node x_i is detectable and the BIT/TE tests apply all the input combinations to the network to completely test the circuit. $P\ (Y_1=1 \cup Y_2=1 \cup \ldots . \cup Y_m=1) | X_i=0 =0$ if the stuck at zero fault on node x_i is not a detectable or the appropriate test pattern is not applied to the circuit inputs. This probability may be between 0 and 1 if the test patterns are applied randomly by the BIT/TE hardware and the fault is detectable. This situation may occur when say a BIT system can't complete all the tests because the test time would interfere with the mission objectives.

Let the probability of a stuck at k error on node x_i be detected given that $X_i=k$ ($k=0, 1$) be

$$P\ (Y_1=1 \cup Y_2=1 \cup \ldots . \cup Y_m=1) | X_i=k \quad =P_{ik}$$

Note that

$$P_{ik}= \begin{cases} 0, \text{ if error } X_i=k\ (k=0,\ 1) \text{ undetectable} \\ 1, \text{ if error } X_i=k\ (k=0,\ 1) \text{ detectable and proper test sequence applied} \\ a, 0 \quad a \quad 1 \text{ if error } X_i=k\ (k=0,\ 1) \text{ is detectable and proper test} \\ \quad \text{sequence may or may not be applied} \end{cases}$$

Now assume the probability of failure of a node x_i is exponential distributed with a failure rate $_i$. Let t denote the mission time hence

$$P\ X_i=0 \quad =P_0(1-e^{-\ _it})$$
$$P\ X_i=1 \quad =P_1(1-e^{-\ _it})$$
$$P\ X_i=2 \quad =e^{-\ _it}$$

Where

$$P_0=P\ X_i=0 | x_i \text{ fails}$$
$$P_1=P\ X_i=1 | x_i \text{ fails}$$

Note $P_0 + P_1 = 1$

The probability of any error occurring and being detected is

$$P\{\text{Fault Detected} \cap \text{Fault occurs}\} = \sum_{i=1}^{n} \sum_{k=0}^{1} P\{X_i = k \cap (Y_1 = 1 \cup Y_2 = 1 \cup .. \cup Y_m = 1)\}$$

$$= \sum_{i=1}^{n} \sum_{k=0}^{1} P\{(Y_1 = 1 \cup Y_2 = 1 \cup .. \cup Y_m = 1 | X_i = k\} \; P(X_i = k)$$

$$= \sum_{i=0}^{n} \sum_{k=0}^{1} P_{ik} P(X_i = k) = \sum_{i=0}^{n} [P_{i0} P_0 (1-e^{-\lambda_i t}) + P_{i1} P_1 (1-e^{-\lambda_i t})]$$

Since no two faults occur simultaneously. The probability of a fault being detected given that it occurs is

$$P\{\text{Fault Detected} \mid \text{Fault Occurs}\} = \frac{P\{\text{Fault Detected} \cap \text{Fault Occurs}\}}{P\{\text{Fault Occurs}\}}$$

$$= \frac{\sum_{i=1}^{n} [P_{i0} P_0 (1-e^{-\lambda_i t}) + P_{i1} P_1 (1-e^{-\lambda_i t})]}{\sum_{i=1}^{n} [P_0 (1-e^{-\lambda_i t}) + P_1 (1-e^{-\lambda_i t})]}$$

The BIT/TE Parameter Fraction of Faults Detected (FFD) is

$$\text{FFD} = \frac{\text{quantity of faults detected}}{\text{quantity of all faults}}$$

Let us assume all nodes may have faults. Thus, the quantity of all faults equals 2n because of a stuck at zero and a stuck at one at each node. Let us assume that all necessary test sequences are applied to the circuit which means $P_{ik} = 0$ or 1 (i.e. 0 if undetected and 1 if detected). The number of detected faults is then $\sum_{i=1}^{n} (P_{i0} + P_{i1})$. Now assume $\lambda_i = \lambda$ and $P_0 = P_1 = 1/2$ (i.e. the failure rate at each node is the same and probability of a stuck at zero is the same as probability of a stuck at one).

Then

$$P\{\text{Fault detected} | \text{Fault occurs}) = \frac{\sum_{i=1}^{n} [P_{i0} P_0 (1-e^{-\lambda_i t}) + P_{i1} P_1 (1-e^{-\lambda_i t})]}{\sum_{i=1}^{n} [P_0 (1-e^{-\lambda_i t}) + P_1 (1-e^{-\lambda_i t})]}$$

$$= \frac{\frac{1}{2}(1-e^{-\lambda t})\sum_{i=0}^{n}(P_{i0}+P_{i1})}{(1-e^{-\lambda t})\sum_{i=1}^{n}[P_0+P_1]}$$

$$= \frac{\sum_{i=1}^{n}(P_{i0}+P_{i1})}{2n} = \frac{\text{quantity of faults detected}}{\text{quantity of all faults}} = \text{FFD}$$

This will be true when all failure rates and the probability of stuck at zero and one is the same. A much better picture of the FFD parameter would however be the statistical one instead of the ratio of numbers.

Example. Consider the digital combinational circuit in Figure 1 and its corresponding truth table in Table 1

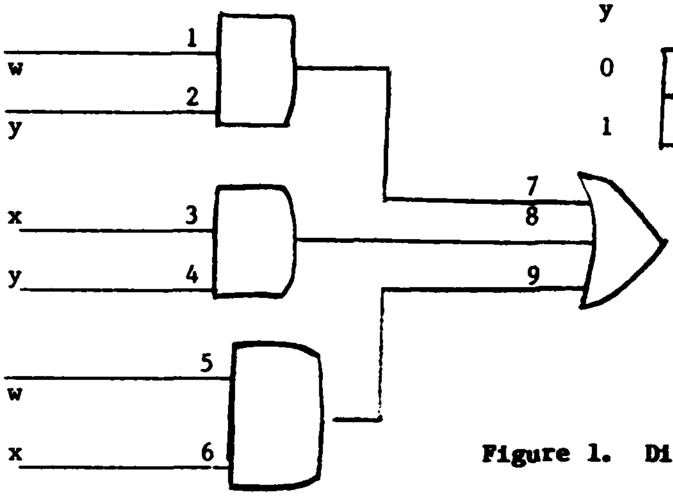


Table 1. Truth Table

y \ wx	00	01	11	10
0	1	1	0	0
1	0	1	1	0

F(w, x, y)

Figure 1. Digital Combinational Circuit

Assume the BIT/TE can apply any or all of the 8 input combinations and the only output is f(w, x, y). The nodes where stuck at one or zero faults may occur are labeled 1 through 10. Assume the failure rate at each of the 10 nodes is the same but the probability of a stuck at zero is ¼ and the probability of a stuck at one is 3/4 i.e. $P_0 = \frac{1}{4}$ and $P_1 = 3/4$. It is possible to show that nodes 5,6, and 9 cannot detect a stuck at zero fault and all other faults can be detected. Therefore $P_{50}=P_{60}=P_{90}=0$ and all other $P_{ik}=1$. Then

$$P\{\text{fault detected} \mid \text{fault occurred}\} = \frac{10 \cdot P_1 + 7\,P_0}{2 \cdot 10} =$$

$$= \frac{10 \cdot 3/4 + 7 \cdot 1/4}{2 \cdot 10} = \frac{43 + 28}{4 \cdot 2 \cdot 10} = \frac{71}{80} = 0.89$$

While $\text{FFA} = \frac{10 + 7}{2 \cdot 10} = \frac{17}{20} = 0.85$

The unequal probabilities for other cases can also change the picture of the effectiveness of the FFA and other measures as well.

3.4 CONCLUSIONS:

The adequacies of some of the other BIT/TE Parameters in the light of statistical observations can be shown to give misleading results, such as the Fraction of Faults Isolated, the Fraction of False Status Indications, and the Fraction of Erroneous Fault Isolation Results. The above analysis could also have been applied to digital systems which have different failure rates for say RAM memory, ROM memory, CPU, interface devices, etc. It is felt that many other parameters should be defined on a statistical basis.

4. ANALYSIS OF CURRENT ANALYTICAL TECHNOLOGY

In this chapter all technologies which have been used in studying different problems in the field of testability and fault tolerance are surveyed and discussed. First, emphasis is directed towards those technologies which are used to tackle different testability and diagnostic problems. Secondly, available procedures and technologies in related disciplines are presented.

4.1 Ad Hoc Testability Techniques and Analysis

The available technologies which were used to investigate the field of testability will be discussed and evaluated in each of the following areas:

- Design of diagnostics
- Evaluation and assessment of diagnostic systems
- Cost design characteristics and design guidelines for testing systems

Discussion of all available technologies and the way they are used to tackle different problems in each area will first be presented and reviewed, then a general evaluation for all techniques which are used in each area will follow.

4.1.1 Design of Diagnostics

In this area, many problems dealing with the designing of different testing procedures and rules are discussed. The problems vary from simple ones dealing with deriving simple rules to be used in determining an efficient testing sequence to diagnose a faulty unit in a designated equipment to a more sophisticated search strategy to optimize the sequence of tests to be executed to find a faulty unit at different levels of repair.

The search in this area, started back in the late fifties when Gluss (1959) tackled the problem of having a fault developed in a system consisting of n modules where each one contains several components. It is required to dictate a search strategy that will optimize the search in some fashion by minimizing a stipulated cost function. Two mathematical models are developed. The first assumes that over-all tests of each module may be performed, and that individual item tests within modules may also be performed. (The search is subject to the constraint that before conducting item tests the faulty module must first be determined by module tests). The second assumes that over-all module tests are not possible, and that penalty costs must be paid whenever the search moves from one module to another. For both models, equations are derived to find the search procedure based upon the relationship between probability of failure and cost or time of testing each module. By solving these equations, an optimum search strategy is derived for the first model only.

Firstman and Gluss (1960) extend the work on the previous models of Gluss, in which the estimation of the probabilities of faults lying in respective modules or components is performed in a different way from that in Gluss's original work: they are computed from component reliability data by manipulation of the component failure rate. Furthermore, consideration is given to fault symptoms that are supplied by weighting the probabilities according to the symptoms information. A mathematical model is derived to find a feasible test sequence to locate the faulty module, then the faulty component in it. The search sequence derived by this model is not necessarily optimal. The search policy derived from the model is based upon the relation between the probability of failure and time required to test each component and each module, as well as the probability that the test fails to detect an actual fault in the module or component tested and the probability that the test finds a fault that does not exist.

The problem of constructing a low cost testing sequence to diagnose the source of an equipment malfunction is tackled by Johnson et al. (1959). They use the information gain theory to provide a figure of merit with which it is possible to construct an efficient testing procedure. If the initial status of the equipment is specified by the a priori probabilities of failure of the individual LRUs, then in any complete testing procedure this initial ambiguity is reduced until the faulty unit is identified at the final state and the ambiguity of this state becomes zero. Therefore, minimizing the average cost of the testing procedure is equivalent to minimizing the average cost per unit ambiguity removed. The cost per unit ambiguity removed can be calculated for each test as a function of the difference between the ambiguity of the state preceding the test and the two succeeding states. This will provide a figure of merit for deciding which test should be done after each state.

In spite of the fact that this approach proves to be logical, simple and easy to use it fails to guarantee an optimum cost sequence and it leads only to an efficient procedure.

Kletsky (1960) demonstrates the validity of the information theory approach suggested by Johnson et al. by studying a standard communication receiver (R-278 B/GR), then he proposes a diagnostic procedure to test it. Kletsky reports that this method requires only simple repetitive calculations and can be easily programmed for automatic computation. The method can be adapted to provide diagnostic procedures appropriate to almost any level of maintenance (organization, intermediate, or depot). Kletsky also indicates that the diagnostic procedure determined by the information theory method can be used as a check-out procedure and the optimum check-out procedure can also be determined using the information theory approach.

Winter (1960) studies the same problem under different restrictions. He considers an equipment in which units can only be tested one at a time, or all at once and where the failure of one unit does not cause the equipment to cease functioning. Winter develops a simple algorithm to detect the faulty units with the minimum expected cost using conditional probabilities and statistical analysis.

Winter derives necessary conditions in order to find an optimal testing sequence by successive permutations of adjoining units using conditional probabilities and statistical analysis. Then he develops an algorithm to optimally detect all the faulty units in the equipment in the sense of minimizing the expected costs. He also finds the optimal test sequence procedure in the case of having only one faulty unit in the equipment using a similar approach.

Chang (1968) tackles the primary isolation problem of finding a sequential testing procedure. He introduces the distinguishability criterion for computing the figure of merit of tests to derive efficient testing procedures. The criterion can be applied to optimize the diagnosability so as to identify failures only to the smallest replaceable unit level. The idea behind the distinguishability criterion lies in the notion of "fault distinguishability". The basic philosophy is that in order to apply a test to distinguish a faulty LRU from a good one and from all other faulty units, the most useful tests are those which distinguish among the largest number of pairs of units. Chang derives an equation for the computation of this criterion and with modification, the criterion can be used in the case of isolating faults to the module level as well as the component level. The criterion proves to be compatible with the concept of information gain if diagnosability is aimed at the module level. The sequential testing procedure which is generated based on the distinguishability criterion proves to yield shorter testing sequences and better resolvability.

Cohn and Ott (1971) present a recursive algorithm to specify an adaptive testing procedure that detects a failure and isolates the faulty component or module while minimizing the expected cost of testing. This algorithm is based on the concept of dynamic programming. The problem is described by tree structures, with nodes labeled by tests and branches labeled by equipment units. Each node of a tree can be interpreted as a state of ignorance, called an ambiguity subset. The ambiguity subset at each node consists of the branches that are descendent from the node. The test applied at a node serves to partition the associated ambiguity subset, thus reducing the ambiguity. The root node, or full subset corresponds to a state of complete ignorance, while at the branches, which correspond to unit subsets and hence where the outcome is determined, there is no further ambiguity. The solution is based on the observation that if for every possible ambiguity subset there can be assigned an evaluation, consisting of the least expected cost of resolving that ambiguity, then the evaluation of the subset of complete ignorance is the cost of the optimal tree. This evaluation function can be computed by a recursion on the number of elements in the ambiguity subsets. The evaluation of any subset is the minimum, over all partitionings, of the expected cost of the test plus the evaluation of the two subsets thus reached. The evaluation of the subset of complete ignorance is the cost of the optimal testing procedure.

Butterworth (1972) considers the system which works if k or more of its n components work. He develops a mathematical model to derive several rules for finding the optimal sequential policies for series and parallel systems of independent LRUs. In the first model a feasible test procedure to determine if the system is working or has failed is developed. This model is solved for the series and parallel systems and under a certain condition for the general k/n system. The solution is based on the relationship between the probability of failure and the average time of removing and replacing LRUs. In another model, a feasible test procedure is derived to locate all failed components for the general k/n system.

Butterworth's rules fail to identify an optimal policy for the simple system where the testing costs are identical for all components. In this case the condition implies that all the components have the same failure probability. However, Halpern (1974) presents a simple adaptive sequential testing procedure for the k-out-of-n system with equal cost of all tests. His algorithm is a heuristic one compared to Butterworth's.

Pieper et al. (1974) develop a step-by-step computerized procedure for generating complete troubleshooting trees which will identify the system's functional unit which is causing observable system malfunction indications. These trees are not expected to be applicable to the piece part level of individual circuits, but to a grosser level of component representation such as an entire functional unit. A computer program (FORTRAN IV) is developed. It inputs information on system data flow, component reliability and cost of available tests. The most efficient sequence of tests to isolate all possible faults is arrived at by using an iterative procedure. The procedure is developed by computing an index of the information gained per unit of cost (IGUC) for each test. The test with the highest IGUC is selected as the first test in the tree. The IGUCs are then recomputed for the remaining tests and the test with the highest IGUC is added as the next step in the tree. The process is repeated until a tree is developed. This tree will isolate all faults. This approach does not guarantee 100% isolation and significant refinements to the technology are suggested to make it operational. However this work proves that computer generation of troubleshooting trees is feasible and could be efficient. Problems might be encountered only when a large numb r of system states and large complex feedback loops exist simultaneously.

Ben-dov (1977) uses the concept of importance of components to develop a branch and bound algorithm to determine the optimal testing policy which minimizes the expected cost of testing a coherent system. Reliability importance of components is studied. The optimal tree is developed to point to the component to be tested first. Based on the results of this test, the search proceeds to the next branch. Subtrees are developed such that at each iteration, the subtree on hand has the lowest bound for the expected cost.

Takami et al. (1978) present a probabilistic model based on Markov processes for a class of series systems which have fault detectors to find component failures where functioning components suspend operation while the system is failed. The problem of allocating detectors with the objective of minimizing the expected loss caused by system failure as well as minimizing the cost of detectors is formulated as a nonlinear 0-1 integer program. The problem is solved easily by hand calculations because the nonlinearity is of a special type.

Sheskin (1977) investigates two related problems in the specification of a BIT diagnostic subsystem for modular electronic equipment where a primary equipment is composed of modular line replaceable units (LRUs), all of which operate independently. Associated with each unit is an a priori probability of being in failure, and it is assumed that the probability of multiple failures is negligible. Whenever the equipment fails, two types of diagnostic tests should be used for the primary and secondary isolations. The BIT automatically executes a sequence of primary diagnostic tests to isolate the group which contains the single faulty LRU. After the execution of the BIT, secondary isolation will be performed by semiautomatic or manual means to locate the single failed unit within a group of LRUs.

Sheskin (1977) formulates the problem of determining a minimum expected cost testing procedure for primary isolation as a probabilistic dynamic program. The problem is divided into stages, such that each stage represents the number of untested elements. The next state is dependent on the probability that the test on the current state will pass or fail. A recursive relationship that identifies the optimum testing sequence at each state, given the optimum testing policies for the subsequent states is formulated. Using the recursive relationship the solution procedure begins by equating the expected values of the terminal states (which correspond to the groups into which the equipment is partitioned) to the expected cost of secondary isolation for these groups. At each state, a set of possible decisions consisting of all the tests which can be performed is considered and the optimal testing sequence at this state is found, until it finds the optimal testing diagram when starting at the initial state.

Under the assumptions that BITs are imperfect in the sense that they will not detect all possible errors in the LRUs which they test, and can also give false alarms by erroneously indicating faults in LRUs which are functioning correctly, Sheskin (1979) develops a hybrid dynamic programming algorithm to determine both the optimum partition of the equipment and the minimum life cycle cost set of BIT which produces this partition. All states of the equipment in this formulation are considered as potential terminal states. A testing sequence can be divided into stages, such that each stage represents the number of untested units. A set of possible decisions at each state consists of all the built in tests which can be performed plus the alternative of performing secondary isolation on that state.

The solution procedure begins by moving backward stage by stage. It starts at stage one in which each state contains a single failed LRU, the desired BIT testing sequence is determined only after completion of the entire recursive algorithm. The backward recursive process ends at the last stage, the single initial stage, where no LRUs have been tested. Since the probability of the initial state is known, all other state probabilities can be obtained. Therefore, starting at the initial state and moving forward executing these forward computations of state probabilities, an optimal testing sequence can be constructed along with the partition into mutually exclusive terminal states which this testing sequence produces. This sequence will minimize the life cycle cost of BIT diagnostic subsystems.

Aly (1979) constructs the same problem which is presented by Sheskin (1979), as a search tree. He presents a branch and bound algorithm to find the optimal sequence of tests to be executed by the automatic BIT diagnostics to isolate a single malfunctioned unit within a group of LRUs.

The search tree consists of nodes and branches. Each node can be interpreted as a subset of tested and untested LRUs. The test applied at a node serves to partition the associated subset, thus reducing the ambiguity. The root node corresponds to the state of complete ambiguity.

Necessary rules for an efficient branch and bound algorithm are derived. They include rules for branching from nodes to new nodes, rules for determining lower bounds for the new nodes, rules for choosing an intermediate node from which to branch next, and rules for recognizing when a node contains only nonoptimal solutions (dominance rules). Then, the branch and bound algorithm is developed and discussed. This approach guarantees finding an optimal testing sequence.

Aly and Elsayedaly (1981) modify the previous algorithm by developing stronger rules to increase the efficiency of the branch and bound algorithm. The algorithm is then programmed and proved to be more efficient than Sheskin's dynamic programming approach. Capitalizing on the computational results of this algorithm, a heuristic algorithm is developed, tested, and compared with the branch and bound algorithm. Even though the heuristic algorithm does not guarantee finding an optimal testing sequence, the computational results indicate that it is faster than the branch and bound algorithm with a very slim sacrifice in optimality and therefore the heuristic algorithm proves to be a good compromise between the ultimate goal of optimality and the problem of time required to achieve this goal. This algorithm has the advantage of finding a near optimal solution in a very short time compared to othpr methods.

Having discussed the available technology in the area of design of diagnostics, the lack of optimization techniques is quite obvious. The trend has always been to try to find a simple procedure using a few important parameters (like failure rate, testing time). This trend has its impact even on the formulation of the problems themselves by imposing many restricted assumptions and/or constraints.

The difficulties associated with the design of diagnostics are clear, also is the need for practical and easy to follow testing procedures. However, Sheskin and Aly proved, by efficiently using optimization techniques (dynamic programming and branch and bound) that it is possible to introduce more advanced techniques to this area and that it is feasible to eliminate some of the imposed assumptions to solve real world problems. Unfortunately, optimization techniques, so far, can be applied only to solve small size problems because of the rapid increase in the solution time with the growth of the problem size. However, using these optimization techniques opens the door to more efficient techniques, though not optimal, which might be more practical for use like the heuristic algorithm prepared by Aly and Elsayedaly.

Also, it is noticed that, even though many techniques were proposed to solve similar problems, there is insufficient computational experience to compare the efficiencies of these different techniques and see how they can be linked together to obtain a superior algorithm.

4.1.2 Evaluation and Assessment of Diagnostic Systems

In this area, problems of evaluating and analyzing diagnostic systems are discussed. These problems deal mainly with two aspects. The first is studying the effectiveness and reliability of the automatic Built-in-Test and/or External Test Equipment System (BIT/TE) as a function of the physical and functional characteristics of the BIT/TE used in the system/equipment. The second is evaluating fault detection/fault isolation (FD/FI). The first available work in this area is by Pliska et al. (1979) who study a diagnostic system which consists of BIT and/or External Test Equipment in order to determine the measures and figures of merit that are required to determine the adequacy of these systems and develop necessary methodologies to analyze and demonstrate these measures. In order to satisfy these objectives five tasks were performed.

a. Collection of data by surveying the available Figures of Merit (FOMs). Detailed mathematical equations are derived to analyze and demonstrate each one of those FOMs. The outcome of this task is used to aid in the identification of additional BIT FOMs or the analysis/demonstration methodologies required for each FOM. The FOMs which are discussed include: fraction of faults detected, fraction of false alarms, fraction of false status indications, mean fault detection time, mean BIT/TE running time, frequency of BIT/TE execution, test thoroughness, fault isolation resolution, fraction of faults isolated, mean fault isolation time, maintenance personnel skill level, BIT/TE maintainability, BIT/TE reliability, BIT/TE availability, mean time to repair, system availability, memory allocated for BIT/TE, and physical characteristic FOMs (e.g. weight, cost, etc.). Each one of these FOMs is categorized according to BIT/TE objectives. Categorization is important because it determines the appropriate set of FOMs that should be specified for a given application and determines which FOMs are interrelated.

b. Evaluating the suitability of the defined FOM as a design specification by taking into consideration the following scoring factors: ambiguity, translatability, trackability, demonstrability, applicability, and uniqueness. Weights are assigned to these scoring factors according to their importance. A simple mathematical model is used to evaluate the FOMs using the scoring factor weights.

c. Developing appropriate analysis techniques for the defined FOMs. These techniques can be divided into three groups: rate dependent techniques, time dependent techniques, and rate and time dependent techniques. The analysis techniques applicable to each FOM are discussed and the required models are developed; all are simple mathematical equations. Formal demonstration tests are used to assess the degree to which certain FOM requirements have been met. These tests are statistical tests based on random variables having certain probability distributions where certain random quantities containing information about the true value of the FOM under consideration are observed and evaluated taking into consideration both the consumer and producer risks.

d. Developing a procedure for determining what BIT/TE FOMs should be specified for given system or equipment objectives. The procedure is based on a guideline methodology using a suggested guidelines matrix and different ranking criteria. Tables are presented to summarize the constraints that must be followed when related FOMs are specified together.

e. Determining how the newly developed BIT/TE FOMs and their associated analysis/ demonstration techniques should be implemented into a maintainability program plan.

Gleason (1981) studies the effectiveness of BIT/TE systems and the implication of the CNDs, RTOKs, and false alarms which are inherent in such systems. He uses the expected number of removals (ENR) that occur per single prime system failure (assuming the application of the BIT/TE system to detect and isolate a failure) as a measure of effectiveness of the BIT/TE system and how effectively the associated test equipment is performing its designated job of fault detection and isolation. This measure is based on four BIT/TE specifications and one maintenance policy factor: BIT/TE fault detection capability, BIT/TE average ambiguity level, BIT/TE misassignment factor, BIT/TE false alarm factor, and maintenance policy removal rate. All these factors are combined together to develop a procedure to evaluate the overall effectiveness of the designated BIT/TE system. This procedure is so general that it can be used at any level of maintenance (organizational, intermediate, depot) and for line replaceable units as well as shop units. This procedure starts by determining the acceptable specification of the BIT/TE, then using a diagnostic event tree, the value of ENR can be calculated. An equation is derived to compute ENR, consequently the average ambiguity level could be determined. These equations are subjected to a sensitivity analysis to ascertain the effects of each BIT/TE specification on the overall test equipment effectiveness parameter (ENR). This analysis is accomplished by selecting a baseline set of test parameters, and then individually changing one parameter, while holding other parameters constant. This provides insight into the overall effect of each parameter on test system effectiveness.

Conley (1980) presents a Failure Modes and Effects Analysis (FMEA) procedure to be used on a complex digital data system where the specification for the system requires that 98% of all failures are to be detected and 90% of all failures are to be isolated to one pluggable assembly. The overall process which evaluates and improves the system's diagnostic capability begins with a preliminary diagnostic prediction. This prediction is based on estimates concerning the effectiveness of hardware and software diagnostic techniques applied to functions in the system. The FMEA approach is then tailored to allow a detailed diagnostic prediction to be performed based on all possible failure modes in the system. From the FMEA data base, the percentage of the system faults, weighted by their respective probabilities of occurrence, which could be detected and/or isolated is readily determined. In addition, the areas where faults could not be detected and/or isolated are identified, thereby indicating the specific areas to address for improving the system's diagnostic capability. The final step in the diagnostics design/evaluation process - fault insertion - verifies the system diagnostic capability by simulating faults through the opening and shorting of test points. Because the FMEA provides test point effects for each failure mode, the percentage of the total number of system failures that are simulated by this fault insertion technique is known. When customized and used in this manner, the FMEA provides for a more accurate diagnostic prediction, an improved diagnostics design, and a maintainability demonstration test which more accurately portrays the system's future maintenance characteristics.

Tuttle and Loveless (1980) study the reliability of the BIT/TE system as a function of the complexity, physical characteristics, and functional characteristics of the BIT/TE used in support of a system. They also study the impact on the operation of the prime equipment due to the failure modes of BIT/TE. A technical discussion of BIT and external testers and their design characteristics is presented. This includes types of BIT, method of activation, method of evaluation, and the effect of operator intervention. The types of BIT studied are comparator, wrap around, signal monitors, and interactive. Manual and computer-initiated BIT are the methods of activation. Three methods for evaluating the results used during the running of BIT are studied: operator, central computer, and unit internal software. The impact on BIT which requires operator intervention is independently assessed. A description of the equipment studied (airborne systems from the S-3A, and C-5A aircraft) and the design data for these systems are also presented.

From the collected field data, the effectiveness of the BIT is evaluated by considering several effectiveness measures: the percentage of system faults which can not be duplicated at the organizational level (CND_O) which were BIT discovered, the percentage of organizational level maintenance over three hours, and the intermediate level can not duplicate (CND_I) percentage. The distribution of organizational level maintenance times is used to obtain a factor indicating excessive maintenance time. A wide range of equipment types and BIT characteristics are evaluated to arrive at relationships which can be used during early planning and design phases for new acquisitions to develop BIT/TE systems. Equipment design factors studied include weight, power, system complexity, parts count, number of cards, number of equipment failure modes and type of equipment.

A statistical analysis of the data relating the LRU design attributes to the effectiveness measures for equipment design factors and BIT characteristics are used to develop a criterion for use in BIT/TE trade-off.

Three levels of data analysis are used. The first provides averages for the characteristics which can be used for quick estimates of individual parameters. At the second level a generalized least squares curve fitting technique is used to obtain the best fit curve for the parameter pairs from among 72 possible first and second order polynominals. The third level of analysis uses multiple linear correlation techniques to provide equations relating the equipment design factors: BIT characteristics, design attributes and effectiveness measures. Only the first and third levels provide useful results.

Horkovich (1981) discusses the importance of developing an efficient methodology to evaluate fault detection/fault isolation (FD/FI) systems, a methodology that could not only identify the existence of problems, but could also provide the evaluator with sufficient information to determine the nature of the problems (faulty FD/FI parameters, lack of FD/FI capability, environmental problems, workmanship problems, software problems, test tolerance, aircraft unique or hardware unique problems). The developed methodology focuses on three basic elements to provide answers to these problems: a single thread closed loop data system, a mean-time-to-repair tool, and relating numbers to meaningful criteria. Each one of these tools is discussed and analyzed in detail. The importance of each tool in identifying and controlling the FD/FI performance is presented. The effect of applying this methodology to E-3A surveillance radar and the F-16 FD/FI systems is reported to be significant. It is also reported that for greater effectiveness, FD/FI systems are to be incorporated during the development and testing cycle and specification parameters should at least include:

a. Percentage of addressable FD/FI

b. Percentage of time correct FD/FI

c. Overall system MTTR

d. CND & RTOK rates

e. Percentage of maintenance accomplished using manual and automatic modes

f. System MTTR model

g. Maintenance man-hours

Linden (1981) studies the effectiveness of BIT/TE and discusses approaches/trends towards highly automated diagnostics. From this discussion, he concludes that: diagnostic specifications are to be written with a clear understanding of the methodologies which can be employed by the contractor in meeting them, occurrences of multiple faults, though rare, should not be ignored, could not duplicate (CND) and retest okay (RTOK) rates are to be specified and should be kept to a minimum. False alarms, CNDs, and RTOKs are explained and their role in determining the effectiveness of BIT/TE are discussed. Test results for E-3A surveillance radar are included to demonstrate the potential magnitude of the problem. Early involvement in the diagnostic system is suggested, also the diagnostic development should go hand in hand with the hardware design in order to be more efficient. The need for 100% diagnostic capability is explained.

From the review of the above studies which have been done in the area of evaluation and assessment of diagnostic systems, it is noticed that the emphasis on all work is to find a valid and reliable procedure to check the effectiveness of BIT/TE system. The use of FOMs to achieve this objective is a good idea, even though many parameters have to be considered and some of them even after being defined are very difficult to assign values to. In addition other FOMs may not be comprehensive, for example, the expected number of removals (ENR) that occur per single prime system failure. Even though this technique takes into consideration the implication of can not duplicates, retest okays, and false alarms, it ignores other factors. Also, it is noticed that some of the so-called methodologies which have been mentioned are simply general logical discussions of the critical parameters of the BIT/TE and their effects on the effectiveness of the system. In general, the techniques used in this area are complemented by statistical analysis (curve fitting, regression analysis) and sensitivity analysis. At the moment, it is hard to say that there is one single technique to evaluate BIT/TE or FD/FI systems. The field is open to more investigation and it requires actually developing different techniques for different systems taking into consideration the characteristics of each system.

4.1.3 Cost Characteristics and Design Guidelines for Testing Systems

In this field, work is mainly related to studying cost characteristics of testing systems by defining cost parameters and developing cost models which analyze the cost aspects of the system. Also general design guidelines for testing specific systems as well as general systems are discussed.

Gaertner (1974) describes the design of the BIT circuitry for tactical FM radios. Several goals to be met in the design are discussed:

a. achievement of fault isolation to a replaceable module/printed circuit card level

b. minimization of BIT size, weight and power consumption

c. elimination of possible interaction with the radio set operation when the BIT unit is in operating, nonoperating, or failure mode

d. continuous on-line monitor and press-to-test mode capabilities for fault detection

e. achievement of fault isolation through press-to-test mode

The following guidelines should be considered in designing BIT hardware for tactical FM radios.

a. development specifications should clearly define the desired BIT characteristics

b. there must be fully integrated design of both the operating circuitry and the BIT circuitry

c. BIT circuitry should be replaced along with the operating circuitry in a given module

d. BIT test sequencing, evaluation, and display circuitry should have a replaceable module by itself and should have self-test capability

Levy et al. (1976) study test procedures and specifications during the depot repair cycle. They develop a method for identifying key maintenance decisions and optimizing tests and test decisions in order to minimize support costs.

The primary emphasis in this study is placed on inertial systems, and in particular maintenance level of the AN/ASN-90 Inertial Measuring Unit (IMU). An analytical model for simulation of the depot and field maintenance process is developed. This model examines alternative tests and test sequencing in terms of system costs and benefits. The costs associated with maintenance of an item of equipment include

a. maintenance costs, depot manpower and material costs, field module costs, manpower, and transport costs between the field and depot.

b. Failed mission costs (the penalty for failing to complete a mission, and the cost of a damaged or lost aircraft and/or crew)

Total cost divided by the number of missions flown provides a measure of performan^e for evaluation of alternatives.

Data is collected in order to validate the simulated model. The methodology includes decision trees, simulation modeling, experimental design, and cost modeling.

Bogard (1980) studies the logistic support cost characteristics of BIT/TE in order to develop guidelines and relationships for use in the development phase of an Air Force electronic equipment program to estimate operation and support costs associated with various types of testers and test subsystems. To achieve these objectives the following steps are taken:

a. The cost elements and related parameters affecting operation and support costs are identified and categorized into four sections: recurring logistics costs, operation costs, maintenance costs, and post production modification costs. Formulas are derived to calculate different costs using cost elements and related parameters.

b. Existing in-house and gcvernment data on a large number of systems, testers and test subsystems are collected to form a data base. This data base is divided into seven general categories: technical data maintenance, training, maintenance, calibration, operation, supply support, and software maintenance. The information collected includes historical data on mean time between failures, MTTR, etc, engineering judgements and experience data, and government and industry cost standards. A summary of this data is presented.

c. The collected data is analyzed in two steps, first, the data for each tester/ test subsystem is applied to cost estimating relationships to generate annual operating and support costs, then a statistical analysis is performed on the basic data and the calculated operating and support costs to yield a series of cost estimating relationships (CERs) which can be used early in the development phase of a program for estimating operating and support costs. A CER is an analytic device that relates the value (in dollar or physical units) of various cost categories to the cost-generating or explanatory variables associated with the categories. Two techniques are employed in this study; engineering and statistical approaches. The engineering approach is based on a deterministic equation which subdivides the cost element into finer factors which are related through cost equations. The element cost of the system or equipment of interest can be computed by substituting the names of the variables into the desired equation. The statistical approach used is a regression analysis technique to develop parametric cost estimating relationships. These relationships take the form of mathematical equations that can be derived through curve fitting techniques applied to the historical cost and physical parameter data. Multiple linear regression is used to generate the CERs.

Three computer models are developed. One model handles the mathematical calculations required to estimate the operating and support costs and to perform the sensitivity analysis on each input variable for each tester. Another model is a modification of an existing multiple linear regression model. The last is written to develop confidence intervals on the predictions for the possible categories.

Heckelman et al. (1981) investigate the effects of architecture, functional partitioning, and module and component features on microprogrammable self-diagnosing capabilities of digital processors. These results are then used to create a set of design guidelines for designing self-diagnosing, fault-tolerant, highly reliable microprocessors, namely monolithic and bit-slice processors using LSI devices. The microprocessor's execution speed, fault tolerance, and mission reliability are also studied.

Two airborne applications are studied: the fly-by-wire flight control processor and the synthetic operature ground map function of an airborne multimode radar signal processor. Both applications are examined to determine the requirements, beginning with mission identification and functional analysis.

The study of these two applications leads to the development of algorithm flow followed by performance analysis of representative tasks and resource sizing in terms of memory, processor speed and complexity as measured by the variety of operations and execution speed. They report that the application of the guidelines strongly influences the design of the self-diagnosing fault tolerant processor. The architectural considerations are of primary importance in the design of a self-diagnosing processor particularly those making extensive use of large scale integrated circuits (LSI).

Besides the previous work, more general studies were done to define tasks that will consider all aspects of automatic testing (on-line, off-line and weapon system testability), with efforts to generate policies and procedures to optimize definition, applications and support of automatic testing hardware and software in the system acquisition management process. Also studies were done to develop system engineering and logistic tools, techniques and guidelines to increase application of automatic testing equipment towards weapon systems.

MIL-STD1591(1977) provides complete guidelines to the designer of BIT equipment to help in recognizing options and selecting the optimal design for a system. The guidelines include general design considerations, BIT design characteristics, evaluation of BIT and optimization of BIT.

4.2 Technology From Related Areas Directly Applicable to Testability

The available technologies from those related areas directly applicable to testability are discussed and explored according to the following fields:

- Evaluation of fault tolerant techniques and network logic procedures.
- Optimization techniques related to electronic logic testing.

Then those techniques which can be adapted to testability areas are discussed to show how they can be used and modified for such adaptation.

4.2.1 Evaluation of Fault Tolerant Techniques and Network Logic Procedures

In the area of testability design several varied areas have been explored. Hayes (1971) considers the design of combinational logic circuits which require a minimal or near-minimal number of tests. For an n-input fanout-free network minimal or near minimal fault detection and location test sets can easily be generated. Unfortunately the fraction of functions that can be realized by fanout-free networks is very small when the number of inputs is large. If a function has some mathematical structure, it may be possible to find a multi-level realization containing fanout which requires relatively few tests. Every linear function can be realized by a cascade function which requires few tests and is such that a complete (and possibly minimal) set of detection tests can be generated without detailed analysis of the circuit. Finally if a function is decomposable into simple functions there often exists a diagnosable multi-level realization. The price paid for the ease of diagnosability of these realizations is the large number of logic levels.

Williams and Angell (1973) investigate the problem of enhancing testability of large-scale integrated sequential circuits by using test points and additional logic to switch the circuit into a second mode of operation, a "test mode". In the test mode the flip-flops are reconnected to form a shift register which provides for ease in testing. However a cost analysis at that time found the method economically infeasible.

McCluskey (1979) looks at many proposed methods of designing for testability for digital systems. First he notes that Bell Telephone Laboratories has come up with an IBM 360 program to estimate the testability of a circuit without test generation. If the testability measure predicts that the circuit will be difficult to test, the circuit can be modified before being released for test generation.

The shift register technique of Williams and Angell is also discussed by McCluskey. It has the advantages of high internal observability and controllability, the problem of test generation for sequential circuits is avoided and very few extra pins are required. The extra circuitry necessary will probably cause some performance degradation, but this should not be significant except for the highest performance systems.

Signature analysis provides simple testing with good (but not complete) coverage. Compact testing (test patterns generated by a pseudo random number circuit) is used to produce a "signature" based on the outputs of the chip being tested. This is then compared with the encoded correct signature.

Finally McCluskey discusses self-testing, that is self-checking hardware built in to the design. In VLSI chips the logic of the chip may be duplicated in complementary form and a comparator used to continuously monitor the signals from the two logic blocks. This design results in very high fault coverage and rapid fault isolation.

Consolla and Danner (1980) seek to develop a guide for testability evaluation and hardware changes of printed circuit boards prior to production release. They work under the constraint that the testability evaluation and correction process should not take longer th 8 to 10 manhours.

Kime (1975) discusses the need for fault tolerant computing and specifically integrated fault-tolerant techniques, i.e. those techniques applied in the design of the system rather than after the fact. One approach integrates test equipment in the subsystems or on the LSI chip itself. Another employs the addition of logic at interfaces between system elements providing the necessary isolation for simplified fault isolation to large units.

Meyer and Rault (1976) discuss a series of papers on the design of fault-tolerant systems. These are in the areas of memory in computing system, "self-synchronized" asynchronous sequential circuits and magnetic tape unit systems.

A fault-tolerant memory design using modular bit swapping to acheive high system availability was presented by Hartwell et al. (1978). The design permits automatic repair of multiple faults without loss of error detection. The technique is directed toward use in a duplex system, although the technique potentially applies to simplex systems.

Hecht (1979) presents two current approaches to fault-tolerant software. In N-version programming a number of independently coded programs for a given function are run simultaneously on loosely coupled computers and the results compared. The success of this technique is governed by the degree of independence that can be achieved in the N-versions of the program.

The second approach is called the recovery block, and can be applied to a more general spectrum of computer configurations including a single computer. A critical feature of the recovery block is the acceptance test, and a number of useful techniques for constructing these are presented. Conclusions derived from a system reliability model for the recovery block that affect the design of fault-tolerant software are discussed.

Many techniques and procedures for evaluating testability have been developed over the last twenty years. Johnson and Brule (1960) define and describe measures of performance and discuss maintenance procedures. They conclude that increasing system mean life is accomplished not by the introduction of redundancy but by increasing maintenance capability.

Seshu (1961) concludes that self-repair of machines may be feasible but the diagnosis conditions are so strict that practical designs will almost certainly be extremely difficult. Some general rules for designing for diagnosability are also given.

Seshu and Freeman (1962) consider the problem of automating the diagnosis of a sequential nonclocked switching circuit. They produce a general purpose program for the IBM 7090 which reads the logical input and produces a testing procedure.

Mandelbaum (1964) defines properties that a function should have to measure the efficiency of a given configuration of output sensors as compared with another configuration on an otherwise same machine. He then notes that those requirements are met by the entropy function of communication theory and gives an example showing this.

Seshu (1965) studies the CSX-1 computer from the point of view of self diagnosis and examining the problems that arise. A diagnosis program on a CDC-1604 is the principal experimental tool. This program is more flexible than the IBM 7090 program of Seshu and Freeman (1962).

A new reduction technique for prime implicant tables is presented by Gimpel (1965). When other techniques fail this may provide a solution. This is useful in finding minimal test sets.

Friedman (1967) gives a heuristic algorithm for handling cyclic prime implicant tables, while Robinson and House (1967) extend Gimpel's reduction technique to covering problems with costs which they illustrate and prove.

A technique by Weisberg and Schmidt (1966) gives an estimate of system reliability for complex systems. They have successfully applied it to various aero-space applications.

Deo (1966) proposes a measure of the self-diagnosability of a computer system. He calls this measure of diagnostic efficiency the "resolution" of the entire system.

Luccio (1966) shows that in minimizing an incompletely specified flow table, nontrivial column reductions may be considered to obtain a low-cost sequential network.

Kautz (1968) uses fault trees to design test schedules for the testing and diagnosis of a small number of nontransient faults in combinational digital circuits. Faults are detected and located precisely or within the confines of a prescribed module.

Preparata et al. (1967) treat the problem of automatic fault diagnosis for systems with multiple faults. The system is decomposed into distinct units, each of which tests a subset of units by means of a given arrangement of testing links. A proper diagnosis can be arrived at for any diagnosable fault pattern. Methods for optimal assignments are given for instantaneous and sequential diagnosis procedures.

The measures accuracy and resolvability of a diagnostic procedure are introduced by Chang (1968). Accuracy is an indicator of the fault detectability of the system's diagnostic procedure. Resolvability is a measure of the quality of the diagnostics and the system repair cost. Both can be computed using diagnostic data obtained from the fault simulation process and used as figures of merit for the diagnostics.

Mayeda and Ramamoorthy (1969) study an application of graph theory to computer diagnosis. The distinguishability criteria in directed graphs is developed and bounds on the number of test points needed to locate faults in a sequential system are derived.

Happ and Sarkisian (1968) develop a program for identification and diagnosis of faults in multi-terminal devices. A combinatorial technique determines the number of z-terminal parent networks. This information is intended to identify and isolate internal faults of the system through an optimal set of external measurements. Following an elementary tutorial, four and five terminal devices are examined. The results are then so formulated as to yield algorithms for computer oriented procedures to identify the complete set of non-redundant configurations of a multi-terminal network. The flowchart of operations suitable for a computer program is presenteα.

Two procedures are presented by Hornbuckle and Spann (1969) for detecting and diagnosing arbitrary single-gate failures in combinational logic circuits. A gate is defined as any multiple-input single-output combinational circuit, and a failure is any detectable transformation of the correct gate function. The testing procedures do not require the construction of a fault table and will locate, to within an equivalence class, the faulty gate and describe its failure.

Three test sets of primary input combinations are defined: the detection set, diagnostic set, and complete set. The first procedure uses the detection and diagnostic sets and requires the application of at most $K^{2m} + K-1$ primary inputs, where K is the number of gates, each with m inputs. This procedure requires considerable computation for each circuit tested. The second procedure uses the complete set and requires the application of at most $(K-1)\ 2^{m+1}$ primary inputs, and all computation is done once for each circuit type. The memory required to store the complete set is proportional to $K^2 \cdot 2m$. The two procedures are adaptive and not necessarily minimal.

Slagle et al. (1970) describe an algorithm which will generate all the prime implicants of a Boolean function. The algorithm is different from those previously given in the literature, and in many cases it is more efficient. It is proved that the algorithm will find all the prime implicants. However, using frequency orderings on literals, experiments with the algorithm show that it usually generates very few (possibly none) nonprime implicants. Furthermore, the algorithm may be used to find the minimal sums of a Boolean function. The algorithm is implemented by a computer program in the LISP language.

A model for the representation of diagnostic test-fault relationships is presented by Kime (1970) which provides increased tlexibility over previous models such as those of Kautz (1968) and Preparata et al. (1967). Kime's model is adaptable to handling large-scale integrated systems. Several forms of the model are given and methods for transforming from one form to another are presented. Procedures are given for assessing the diagnostic capability of the test set and theorems are presented which give necessary and sufficient conditions in terms of the model for diagnosability with and without fault repair. Finally, the model is compared to a number of existing models to demonstrate its flexibility.

It can be shown that a functionally connected system can be represented by an acyclic SEC (single-entry single-exit connected) graph for the purpose of diagnosis. Based on this fact, Nakano and Nakanishi (1971a) present a study on internal test terminals required for diagnosis in relation to the structure of the graph. The equivalence relation of graphs and a procedure for determining a set of internal test terminals are developed. Internal test terminals for a class of systems represented by a special planar acyclic SEC graph are also discussed.

Ramamoorthy and Mayeda (1971) note that in their previous work they consider the application of graph theory to represent and analyze a computer system. By such analysis they show that faults can be detected and located by means of strategically placed test points within the system. Next they present an alternative technique to computer system diagnosis in which the flow of signals within the system is blocked or unblocked by controlling a set of blocking gates. A method of deciding the maximum distinguishability (fault isolation) of a given system is given. Finally they construct an algorithm to determine the optimal location of blocking gates for maximum distinguishability of faults within the elements of the system under arbitrary cost constraints.

Du (1972) explains that in switching theory the covering problem arises in many situations, those of finding minimal fault detection or location test sets for a combinational circuit being among them. In very large problems, where integer programming becomes inefficient, approximate algorithms must be used to find nearly minimal solutions. Du presents an easy way to find a lower bound for the size of a minimal solution of the covering problem.

Scola (1972) discusses the on-line testing system of the Honeywell Series 6000 computer system. The total Series 6000 system is oriented toward optimizing user availability with concurrent maintenance functions. The major features are on-line test diagnostic error visibility and preventive and corrective maintenance. Various portions of the system can be devoted to routine preventive maintenance checks while running user programs. Spot diagnostics can test and diagnose portions of the input-output, communication and central system interlaced with, but not conflicting with, user operation.

Hakimi and Amin (1974) extend the work of Preparata et al. (1967) on the capability of automatic fault diagnosis of a system of n units. A system is t-diagnosable if given the test outcomes all the faulty units can be identified provided the number of faulty units does not exceed t. Hakimi and Amin give necessary and sufficient conditions for a system to be t-diagnosable.

Liguori (1974) discusses digital simulation for circuit testing and design. He gives some applications and limitations of a few of the software tools available for combinatorial logic digital devices.

Akers (1974) presents a method for converting problems in fault diagnosis into ones involving coloring (labeling) the nodes of a graph. Starting with a combinational logic network, it is first converted to its NOR-gate equivalent network. A graph theorist describes this as a directed, acyclic graph. A test is defined as a labeling of each node with either 0 or 1 such that no 1-nodes are adjacent, and every fan has at least one 1-node. If the labels are thought of as colors, any test set with these properties is a proper coloring of the nodes of the graph.

Likewise it is shown that many other concepts and results of graph theory have direct counterparts in fault diagnosis. Specific fault diagnosis problems examined include exercising tests, fanout-free networks, test point insertion, sensitized paths, and fault test generation.

Susskind (1973) notes that the lack of test points in LSI (large scale integrated) circuits, the need for efficient test procedures, and increased need for complete testing of electronic equipment have increased the interest in techniques for detecting and locating failures in complex digital networks. The techniques covered by Susskind are economically feasible only for networks of modest size (hundreds of gates). The balance of the article deals with structure tests which are lengthy though complete as opposed to function tests which are feasible for large systems but are usually not complete.

Although the most universally accepted fault model is the stuck-at (SA) model, it is not clear how well the model fits LSI circuits. Faults such as shorting between adjacent conducting lines and intermittent faults are not covered by the SA model. The problem of multiple faults also can not be ruled out especially in the case of production testing.

For combinational logic, path sensitization using Boolean difference and the D algorithm method provide tests based on the SA model. For the problem of multiple faults an overview of the SPOOF algorithm is given.

For sequential networks the three major ways of finding tests are (1) by verifying functional characteristics, (2) by translating the network into the related iterative circuit, and (3) by verifying the state-table for the given network. Only the first two have gained practical acceptance. The fundamental cause for the difficulty in finding tests for sequential circuits is the fact that the state variables are not available for inspection when a sequential network is tested. Much can be done in the areas of design and layout to improve this.

Nakano and Nakanishi (1974) use graph theory to propose a method for the detection and location of a multiunit fault in a system. The method requires only a slight increase in the number of internal monitoring terminals over the number required for the 1-unit fault diagnosis. A graph representation of a system initially leads to a rectangular diagnostic matrix. An algorithm is developed for constructing a square reachability matrix from the diagnostic matrix. A graph derived from the reachability matrix permits diagnosis of multiunit faults.

Hakimi (1973) presents a summary of the previous work that has been done using a graph-theoretic approach to find conditions for a system of units to be t-diagnosable.

Allan et al. (1975) present a theorem from which all previous work on systems of n units which test each other (such as t-diagnosability) can be derived.

Minimization of the number of states of a sequential machine is important for reasons of fault detection and fault tolerant design. Rao and Biswas (1975) give a simple and efficient method for the minimization of incompletely specified sequential machines. The central theme of the new method is to weed out such of those compatibles which cannot be members of any minimal closed cover and further ignore a substantial number of compatibles, elimination of which does not preclude finding at least one minimal closed cover. The tests proposed to acheive this objective are extremely simple and are easily implemented at the very first stage in the process of minimizing an ISSM. As a consequence, we only have to deal with a relatively small set of compatibles. A lower bound for the cardinality of the minimal closed cover is proposed and a technique to find it is presented. The rank of a compatible is defined and it is shown that ordering the compatibles in accordance with their rank reduces the amount of work involved. An improved technique of generating prime closed sets is proposed which converges faster to the solution.

The methods proposed by Rao and Biswas are simple, efficient and systematic. From the recursive nature of the procedures developed, it is evident that the methods are programmable. For small and medium sized machines, the methods can be used for hand computation as well.

Diagnosability without fault repair of a digital system containing at most t faults is considered by Russell and Kime (1975). A system-level diagnostic model is employed. The model is to an extent independent of the means used to implement diagnostic procedures, i.e., whether the tests are accomplished via hardware, software, or combinations thereof. Two parameters, the masking and exposure indices, are defined. Conjoined with the previously defined closure index, the parameters fundamentally characterize the capability for executing valid tests in a multiple-fault environment. Necessary and sufficient conditions for a system to be t-fault diagnosable without repair are derived in terms of these parameters.

Examples are presented to illustrate the application of the model for systems close to those encountered in actual practice. From the examples it can be noted that the levels of diagnosability particularly beyond 1-fault diagnosability are not generally obtained without a substantial amount of redundancy in the hardware. Thus, in general the most useful application of the model appears to be in the system design stages in which the system is to be configured to provide a specified level of diagnosability. It appears that diagnosability at a high level is not likely to be easily achieved by an after-the-fact effort which does not allow for substantial alterations or additions to the system hardware.

Kohavi and Berger (1975) are concerned with the problem of generating minimal experiments to locate and diagnose faults in combinational tree networks. The procedures presented, although valid only for tree networks, generate the required experiments directly from the network structure, without using a fault table. A fault detection experiment refers to a set of tests leading to a definite conclusion as to whether or not the network operates correctly for all input combinations. The procedures yield minimal experiments when using adaptive testing techniques and yield a bound on the length of the experiments for preset testing techniques.

The paper by Breuer et al. (1976) deals with the problem of identifying multiple stuck-type hardware failures in combinational switching networks. The cause-effect equation for representing faulty circuit behavior is employed. They introduce the concept of solving simultaneous equations over check point variables. These check point solutions are studied in detail, from which one can calculate the function realized by a faulty circuit. An on-line testing procedure for constructing a test set for identifying a specific fault in a circuit to within an equivalence class is outlined. This procedure eliminates the need for precalculating a fault dictionary, which in many instances can be quite advantageous. Also outlined is how to apply these techniques to the following problems: identifying redundancy, determining the set of faults not detected by an arbitrary test set, and constructing a complete fault dictionary.

Maheshwari and Hakimi (1976) are concerned with automatic fault diagnosis for digital systems with multiple faults. Three problems are treated: 1) Probabilistic fault diagnosis is presented using the graph-theoretic model of Preparata et al. (1967). The necessary and sufficient conditions to correctly diagnose any fault set whose probability of occurrence is greater than t are developed. Some simple sufficient conditions are also discussed. 2) A general model that contains as a special case the graph-theoretic model is developed. Conditions for T-fault diagnosability are given. 3) Finally, sequential T-fault diagnosability is considered. Existence of a class of systems requiring as little as n + T - 1 tests is shown. This improves significantly upon the previously best known class of systems that required n + 2T - 2 tests for sequential T-fault diagnosability.

The problem of automatic fault diagnosis of systems decomposed into a number of interconnected units is considered by Barsi et al. (1976) by using a simplified version of the diagnostic model introduced by Preparata et al. The model is supposed to be a realistic representation of systems where each unit has a considerable computational capability. For any system of n units whose set of testing links is given, necessary and sufficient conditions for t-diagnosability are presented in both cases of one-step diagnosis and diagnosis with repair, and it is shown that the procedure for diagnosis with repair has very small complexity. The problem of optimal assignment of testing links in order to achieve a given diagnosability is also considered and classes of optimal t-diagnosable systems are presented for arbitrary values of t in both cases of one-step diagnosis and diagnosis with repair.

Hayes (1976) notes that logic circuits are usually tested by applying a sequence of input patterns to the circuit under test and comparing the observed response sequence R bit by bit to the expected response R_0. The transition count (TC) of R, denoted c(R), is the number of times the signals forming R change value. In TC testing c(R) is recorded rather than R. A fault is detected if the observed TC c(R) differs from the correct TC c(R_0). General methods are presented for constructing complete TC tests to detect both single and multiple stuck-line faults in combinational circuits. Optimal or near-optimal test sequences are derived for one and two level circuits. The use of TC testing for fault location is examined, and it is concluded that TC tests are relatively inefficient for this purpose.

Toida (1976) introduces the concept of redundant tests in relation to the diagnosability of a system. If the addition of a test does not improve the diagnosability of a system the test is called redundant. It is shown that if at least one test is nonredundant, then the previous algorithms by Hakimi and Amin (1974) and Allan et al. (1975) to determine the diagnosability can be further improved. How and when the diagnosability of a system can be improved by the addition of an extra test is also shown.

The problem considered by Koren and Kohavi (1977) is generating sequential decision trees for fault diagnosis in digital combinational networks. Since in most applications of the decision tree the final conclusion will be that the network is failure-free, we are interested mainly in decision trees containing minimal fault detection paths. Such a procedure will reduce the cost of verifying the proper operation of the network.

The faults under consideration are assumed to be single, permanent, stuck-at type faults. A priori probabilities are assigned to the nonequivalent faults and the generated decision tree is based upon these probabilities. It is suggested in this paper that the a priori probability P_i assigned to the fault f_i should be proportional to the number of faults in the equivalence class of f_i.

A procedure for generating the required decision tree for fanout-free networks is presented. The procedure generates the tests directly from the structure of the network instead of selecting them from a given fault table. The generalized decision tree contains a minimal detection path, i.e., a minimal number of tests required to locate the failure-free network. The decision tree yields a nearly minimal weighted average number of tests required to locate a fault. The average is weighted by the a priori probabilities of occurrence of the faults. A lower bound for this average is derived enabling adequate evaluation of the generated decision tree.

Fujiwara and Kinoshita (1978a) are concerned with probabilistic fault diagnosis of digital systems. A graph-theoretic model of a diagnosable system introduced by Preparata et al. (1967) is considered in which a system is made up of a number of units with specified probabilities of failure. Necessary and sufficient conditions are obtained for the existence of testing links (a connection) to form probabilistically t-diagnosable systems with and without repair. Methods for connection assignments are given for probabilistic fault diagnosis procedures with and without repair. They note Maheswari and Hakimi (1976) gave the necessary and sufficient condition for a system to be probabilistically t-diagnosable without repair. Then they show the necessary and sufficient condition for a system to be probabilistically t-diagnosable with repair.

Cox and Carroll (1978) develop a memory array reliability model that can be applied to a wide range of memory organizations including random-access memories (RAM) and read-only memories (ROM). The model is particularly useful for computing the reliability of fault-tolerant memories that employ techniques such as hardware redundancy, error-correcting codes, and software error-correcting algorithms. The model accommodates the effect of faults masked by data.

Fujiwara and Kinoshita (1978b) analyze the computational complexity of system diagnosis. They show that several problems for instantaneous and sequential fault diagnosis of systems are polynomially complete and that for single-loop systems these problems are solvable in polynomial time.

Vink et al. (1978) present the reduction of covering closure (cc) - tables using multiple implication. Closure columns are introduced which are multiply implied and the effect of multiple implication is discussed: a reduction of cc-tables and a simplification of some reduction rules.

Meyer and Masson (1978) give a new diagnosis algorithm for determining the existing fault situation in a symmetric multiple processor architecture. The algorithm assumes that there are n processors, each of which is tested by at least t other processors, and at most t of which are faulty. The existing fault situation is always diagnosed if $n \geq 2t + 1$ and, in some cases, can still be diagnosed if $n < 2t + 1$. The implementation of the algorithm is straightforward and suitable for microprocessor applications.

A procedure is developed by Tasar and Ohlef (1979) for combining the structural fault detection coverage of a self-test program, designed to test a digital computer, with the probability of occurrences of all the faults which have been analyzed to find the coverage. Using this procedure, the combined coverage is calculated for an existing self-test program designed to test the central processing unit (CPU) of a real-time control computer. The theory, application, and results of the analysis are presented.

McPherson and Kime (1979) are concerned with the diagnosis of faulty parts in digital systems, including both the detection and location of such parts. The system model presented in this paper considers two levels: the part level at which detectability and diagnosability are defined, and the fault level at which testing is performed and at which functional units or portions thereof are defined. Parameters are defined and used in determining conditions for t-part detectability, t-part diagnosability without repair, and t-part diagnosability with repair. Several examples are presented with the development of the model and derivation of results. These examples illustrate the advantages and limitations of this model.

Agarwal and Masson (1979) note that to efficiently perform the fault analysis of digital networks it is necessary that pertinent fault interrelationships be utilized. However, determining these fault interrelationships can entail an analysis which is quite complex and thereby reduces the overall advantage of utilizing the gained insights in a fault analysis process. They suggest an approach to establishing the existence of a certain fault interrelationship relative to test set coverage in tree networks which is based only on the form of the output function. A procedure is given for generating a form expression (called L-expression) corresponding to that function. A theorem is stated regarding the interpretation of these form expressions relative to test set coverage.

A new measure of system diagnosis t/s diagnosability, originally proposed by Friedman, is used by Karunanithi and Friedman (1979) to study the diagnosability of digital systems. This new measure incorporates the concept of possible replacement of fault-free units in system repair, whereas the previous measures have only considered the replacement of faulty units. Two categories of the new measure, one-step t/s diagnosability and sequential t/s diagnosability, are investigated. Two canonical classes of systems, single loop systems and $D_{\delta A}$ systems are examined based on these two categories of diagnosability. For each system class, the necessary and sufficient condition for one-step t/s diagnosability is obtained and related to some previous results on t-fault diagnosability; also, an efficient one-step t/s repair procedure is presented. For both these system classes, optimal one-step t/s diagnosable system designs, which minimize the number of units and test links, are considered. Several sequential diagnosis strategies are presented for each system class. For all these diagnosis strategies optimal system designs are also considered. Finally, all the diagnosis strategies are compared and the tradeoff between the number of units replaced and the number of test iterations performed is discussed.

From the field of medicine Swets et al. (1979) discuss the evaluation of diagnostic systems. They claim the current methods of comparing diagnostic systems are inadequate because they fail to accurately model the decision process. The method presented they claim has overcome these shortfalls.

Two radiologic techniques - computed tomography and radionuclide scanning are to be compared. The procedure utilizes real cases and real diagnostic tasks where verification of the presence or absence of a brain tumor has been verified by autopsy or by survival with no symptoms for 8 months. Following a statistically controlled study the results are compared using relative operating characteristic (ROC) analysis (from the general theory of signal detection). The ROC is a curve showing the various trade-offs existing between proportions of true-positive and false-positive responses, as the decision criterion is systematically varied, for a given capacity to discriminate between positive and negative cases. The ROC may form the basis for an evaluation of the usefulness of a diagnostic system. The ROC is a means of determining the response probabilities appropriate to the best available estimates of the values, costs, and event probabilities that inhere in the relevant diagnostic and therapeutic context.

Abraham and Thatte (1979) note that a new approach to testing microprocessors is to model their behavior at a register transfer level, describe the effects of failures at a functional level, and to derive tests based on these higher level models. This paper describes an attempt to quantify the fault coverage of these test by detailed simulation at the logic level with single stuck-at faults. The fault coverage for the particular microprocessor simulated was found to be excellent.

New and extended algorithms are proposed by Allen and Rao (1980) for the synthesis and analysis of fault trees which allow the analyst to focus his attention upon the system's behavior. The algorithms have been applied to a major failure analysis performed upon a chemically active, fluidized bed coal/oil gasification unit. Trees containing 500 gates were synthesized and analyzed.

Rosenthal (1980) describes some kinds of fault tree analysis for which cut set enumeration is inadequate. Modularization leads to more efficient computer programs, and also identifies subsystems which are intuitively meaningful. The problem of finding all modules of a fault tree is formulated as extension of the problem of finding all "cut-points" of an undirected graph. The major result is a FORTRAN program which can find modules of a 1000-event fault tree in a fraction of a second. A generalized module is defined.

In a paper by Malek and Liu (1980) graph theory models applied in fault diagnosis and fault tolerance are surveyed. The models are classified, and their basic features are reviewed. A self-diagnosable and fault tolerant model is characterized, and its applicability for computer systems is examined.

Freedy and Lucaccini (1980) consider training using adaptive computer aided instruction. The Adaptive Computer Training System (ACTS) focuses on improving and sharpening higher-order cognitive skills in electronics trouble shooting. ACTS incorporates an adaptive computer program which learns the student's diagnostic and decision value structure, compares this to that of an expert, and adapts the instructional sequence so as to eliminate discrepancies. An expected utility or multi-attribute utility model is the basis of the student and instructor models which, together with a task simulator, form the core of ACTS. The student model is dynamically adjusted using a trainable network technique of pattern classification. The training content and problem presentation sequence are generated with heuristic algorithms. ACTS is implemented on an Interdata Model 70 minicomputer and uses interactive graphics terminals.

A preliminary study was performed with two groups of six subjects each. One group was trained with ACTS the other using the actual circuits. The results were extremely promising. It is anticipated that in the near future studies will be undertaken in the operational training environment.

Pau (1980) discusses the application of pattern recognition to failure analysis and diagnosis. Basic concepts of failure analysis and diagnosis include: failure, degradation, failure mode, failure detection, failure localization, failure diagnosis, analysis and monitoring. The effects of failure analysis and diagnosis on the system reliability and survivability are discussed. Errors of the diagnostic system are explained including incorrect diagnosis, false alarm, and missing a failure.

Application of pattern recognition to failure diagnosis and performance monitoring is then considered. Four problems are examined: pattern measurement, learning, feature extraction and classification. For each problem, the specific aspects met in applying pattern recognition to failure analysis and diagnosis and the pattern recognition methods used are reviewed. Finally, the publications describing some major implementation are surveyed.

Goel (1981) notes that the D-algorithm (DALG) is shown to be ineffective for the class of combinational logic circuits that is used to implement error correction and translation (ECAT) functions. PODEM (path-oriented decision making) is a new test generation algorithm for combinational logic circuits. PODEM uses an implicit enumeration approach analogous to that used for solving 0-1 integer programming problems. It is shown the PODEM is very efficient for ECAT circuits and is significantly more efficient than DALG over the general spectrum of combinational logic circuits. A distinctive feature of PODEM is its simplicity when compared to the D-algorithm. PODEM is a complete algorithm in that it will generate a test if one exists. Heuristics are used to achieve an efficient implicit search of the space of all possible primary input patterns until either a test is found or the space is exhausted.

Various models of fault-tolerant self-diagnosing computer systems are presented by Risse (1981). The model introduced first by Preparata et al. (1967) is now generalized in the sense that each test result is evaluated by a set of units instead by a single one. Conditions for such systems to be t-diagnosable are given. Existing systems like PLURIBUS serve as examples.

4.2.2 Optimization Procedures

In the design of combinational diagnostic testing procedures for a large digital system, some redundant tests are expected. Chang (1965) describes an algorithm for selecting a good (locally optimized) set of diagnostic tests which contains no redundancy. The algorithm will in general tend to give a "fairly good" set of test patterns, but is not guaranteed to be absolutely minimal. An overall optimization scheme is desirable but seems impractical. The procedure described can be used either to yield a set of diagnostics which loses no resolution from the full set, or to yield a smaller set with some loss in resolution.

Hadlock (1967) presents a method of extending Chang's work to find a test set that will be minimal. The problem is formulated as the prime implicant problem and solved with existing methods. It is guaranteed to yield the minimal test set.

The problem considered by Powell (1969) is the selection of a subset of diagnostic test inputs for combinational circuits. The selected subset of tests will diagnose a single fault to the package level, i.e., until the package which contains the fault is determined. The procedure in obtaining this subset makes use of information provided by multiple outputs, and through a local optimization technique provides a near-optimal global procedure. The local optimization technique weights the tests according to the degree to which they partition the possible faulty packages. The test that provides the greatest partitioning in conjunction with previous selected tests is added to the subset of diagnostic tests.

Preparata (1969) models the diagnosis of digital systems as the recognition of distinct binary error-free patterns. Specifically, if for a given fault condition, the pass or fail responses to a set of applied tests are recorded as a column of a matrix M, a test schedule of length k is a subset of the rows of M which preserves column distinguishability. Since the determination of a minimal test schedule is a formidable problem for moderately complex networks, it appears desirable to have guidelines for the evaluation of heuristically or suboptimally computed test schedules. One such guideline is the median $\overline{k}_{min}$ of the minimal test schedule k_{min} over the set of all binary matrices M: while in general $[\log_2 m] \le k_{min} \le m - 1$, this paper shows that $\overline{k}_{min} < [2 \log_2 m]$, that is, for most practical cases, $\overline{k}_{min}$ is much closer to the lower bound $[\log_2 m]$ than to the upper bound $(m - 1)$.

Nakano and Nakanishi (1971b) represent a functionally connected system by an acyclic SEC graph from the viewpoint of diagnosis. It is shown that the upper directed cutset in an acyclic SEC graph is particularly useful in system diagnosis and, in particular, an estimate of the lower bound on the number of internal test terminals needed for sys^tem diagnosis can be derived. A procedure for determining a set of internal test terminals for system diagnosis is also developed.

A terminal stuck fault in a logic network is represented in Weiss (1972) by one or more stuck-at-1 or stuck-at-0 faults on the n input lines or single output. It is shown that for $n \leq 5$, a least upper bound on the test length is n+1, and for n>5, an upper bound is 2n-4. A greatest lower bound is 3, for all n>1. The upper bounds are based on a maximum size alternating 1-tree in the n-cube representation of the function. Of the more than 600,000 equivalence classes of functions of n variables, $n \leq 5$, only one does not have an n-edge alternating 1-tree. An algorithm is proposed for constructing tests based on alternating 1-trees.

Nakano and Nakanishi (1972) give necessary and sufficient conditions for a set of internal test terminals to be 1-distinguishable for the identification of faulty units in a system comprised of a set of units which are functionally connected. That is, the paper proves that the conventional conditions constitute necessary and sufficient conditions only for certain structures and shows that another condition must be added for the conditions to be general.

Based on the newly obtained conditions, the previous papers of the authors are reexamined and necessary modifications are made. The essential steps of the algorithm remain unchanged in that in the determination of test terminals the absolutely necessary nodes are found and if they are not 1-distinguishable, then the problem is solved as a covering problem. The solution of the covering problem in the new method is more complex because of the addition of a new condition.

Halpern (1974) divides a system and its components into only two states: complete success or complete failure. The components' states are random variables and the system's state depends deterministically on the states of its elements. This paper assumes the state of the system is unknown and presents a sequential testing procedure of the components in order to determine the system's state. The procedure minimizes the expected number of necessary tests for a wide class of systems. The procedure is needed when the system is entirely or partially consumed upon its use, e.g., the firing of a missile, and one wishes to know the system's state without actually operating the system.

4.2.3 Adaptations of Available Technology to Testability Areas

Some of the above work could be considered as a basis for further research in the field of self-diagnosis systems. One such candidate is that of Preparata et al. (1967) who propose a graph-theoretic model of digital systems for the purpose of diagnosis of multiple faults. In this model a system is made up of a number of units. Each unit is assumed to be tested by some other units. A test outcome classifies the tested unit as faulty or nonfaulty, the test being unreliable i the testing unit itself is faulty. In order to diagnose the system a sequence ot tests is performed. In each test a unit tests another unit to find if the tested unit is faulty or fault free. After testing each unit of the system in some sequence, a set of test outcomes is obtained. From this set of test outcomes a central unit determines which units are faulty.

A system S may be represented by a digraph G consisting of set V of vertices and a set E of ordered pairs of distinct vertices of V. An ordered pair $(V_i, V_j) \varepsilon E$ is an edge of G that is directed from V_i to V_j. The vertices of G correspond to the units of S and $(V_i, V_j) \varepsilon E$ if and only if V_i tests V_j in S. The test outcomes may be represented by assigning a weight a_{ij} to each edge $(V_i, V_j) \varepsilon E$.
Consider the situation depicted in Figure 2 where a network of eight units is presented. The units are assigned in a designated manner to test each other. The outcomes of the tests are shown as weight a_{ij} on the various arcs (V_i, V_j) corresponding to these tests, where $a_{ij} = 1$ if unit V_i finds unit V_j to be faulty and $a_{ij} = 0$ if unit V_i finds unit V_j to be nonfaulty. If V_i is faulty then the outcome a_{ij} is unreliable. Assuming that all n units have the same (a priori) probability of being faulty and this probability is less than 1/2, and assuming that the number of faulty units does not exceed t, Preparata et al. show that to identify the faulty units (from the test outcomes), it is necessary that $n \geq 2t + 1$ and each unit be tested by at least t other units.

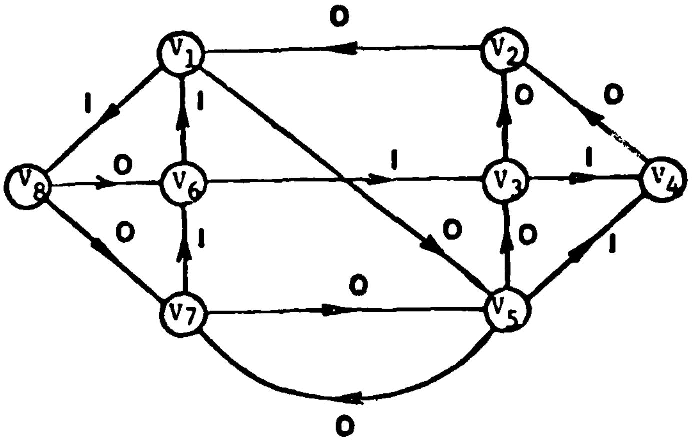


Figure 2. Network of Eight Units

A system S is called t-diagnosable if, given the test outcomes (a_{ij}) all the faulty units can be identified provided the number of faulty units does not exceed t. In their correspondence, Hakimi and Amin (1974) prove that if no two units in S test each other, then the preceeding necessary conditions are sufficient for S to be t-diagnosable.

Having studied the graph theoretic approach to the problem of automatic fault diagnosis, it is noticed that this approach can be slightly modified to tackle the problem of automatic fault diagnosis by considering the automatic BIT as one of the units where this unit is the only one capable of testing all other units while no other unit can test this unit. Furthermore, the following modifications can be implemented separately or together to strengthen the model:

a. The problem is tackled under the assumption that all units have the same probability of being faulty. This assumption should be relaxed in order to make the problem more realistic and probably this can be done with minor modifications.

b. The problem is formulated to consider multiple faults (t faults) which is very general. However, in dealing with the automatic diagnostics, it would be more practical to consider the case of having only one fault. This minor modification might help in finding a reliable solution to the problem.

c. Costs associated with each test were ignored. Inclusion of costs in the formulation might imply a major modification. However they can't be neglected in a variety of applicable problems.

d. Even though a new approach (graph theoretic) to the problem of automatic fault diagnosis is presented, no explicit algorithm for identifying the faulty units was obtained. Thus finding an efficient algorithm for identifying the faulty units, in general, remains an open problem.

e. Including the automatic BIT as a unit in the formulation enables us to consider its probability of failure or false alarm which was ignored in most of the literature dealing with design of optimal sequences of tests to be applied by the BIT.

As it was mentioned above, Sheskin studied the problem of determining the cost-effective design of fault isolation procedures using the built-in test (BIT) diagnostics subsystems for modular electronic equipment. He describes the problem using a network and explains how a dynamic programming approach can be implemented to find the optimal sequence of tests to be executed by the BIT. Even though Aly and Elsayedaly proposed an efficient branch and bound algorithm to solve the same problem, this area is still wide open for further research and modifications.

The problem should be modified by taking into consideration the following aspects.

a. Introducing the concept of fault detection/fault isolation balance into the formulation of the problem. The above analysis of the problem assumes that it is known in advance that one of the unit has malfunctioned and the study starts from here. However the fault detection/iault isolation balance can't be ignored, since the importance of false alarms is proven in current research dealing with BIT. Hence considering the probability of false alarms in the analysis of fault isolation is too important to be excluded. Therefore it should be included in any sensitivity analysis to determine the optimal combination of fault detection/fault isolation within a certain accepted level of significance or within an accepted value of risk. This balance of fault detection/fault isolation within an accepted value of risk is more general, reliable and applicable than considering only fault isolation without considering fault detection at the same time.

b. Even though the previous models consider the secondary isolation in the intermediate level, the cost of the secondary isolation was still assumed to be known and the possibility that when testing the equipment in the intermediate level no failed unit will be recognized was ignored. So, the possibility of RTOKs was excluded. Knowing the importance of RTOKs and their effect on determining the optimal sequence of tests to be executed by BIT, more work should be done to find out the cost of the secondary isolation taking into consideration the transition from the organizational level to the intermediate level as well as all probabilities and risks involved in the decision making process.

The covering problem arises when finding minimal fault detection and minimal fault location test sets. A cover will ensure complete (100%) testing of all faults, while a minimal cover will test all faults with the minimum number of tests possible. The covering problem has been tackled in several disciplines. Gimpel (1965) discusses it with relation to determining the simplest sum-of-products expression for a Boolean function.

First the prime implicants must be determined. Procedures for this have been described in the literature. Given that the prime implicants have been found, Gimpel considers the covering problem. The covering problem is a pair (S,R), where S is a finite set of elements called columns and R is a collection of finite subsets of S called rows. A row is said to cover a column if the column is contained in that row. A cover is a subcollection of R whose union is S. A minimal cover is a cover of minimum cardinality. An irredundant cover is a cover of which no proper subset is a cover. A solution to a covering problem is any minimal cover. A prime implicant table (or incidence matrix) of a covering problem is a rectangular matrix of x's and blanks with the following property: there is a one-to-one correspondence between the rows of the table and the rows of the covering problem, and between the columns of the table and the columns of the covering problem, in such a way that a row covers a column if and only if it appears at the intersection of the associated row and column.

A reduction technique is a technique which, when applied to a given covering problem, can yield a new covering problem so that a solution to the former can be constructed from a solution to the latter. It is assumed that the reader is familiar with three classical techniques: row dominance, column dominance, and the removal of essential rows. The rule by which a solution to the original problem can be obtained from a solution to the new one will be called a conversion rule. A minimal cover for the original table can be obtained from the solution to the new covering problem by carrying out the associated conversion rules.

The classical reduction techniques are limited in the type of problem that can be solved. It is suggested that supplemental reduction techniques need to be developed. The one presented by Gimpel is limited to problems having at least one column covered by exactly two rows. This new technique, like the old, cannot be regarded as affording a total or complete solution for all covering problems. Rather, reduction techniques are always used in an auxiliary capacity with some general algorithm, e.g., row branching, p-function multiplication, or integer programming.

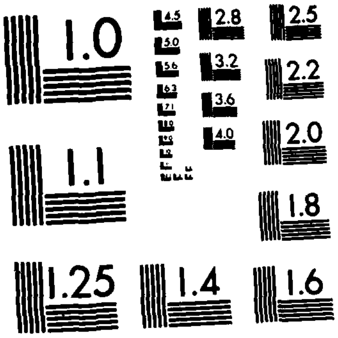
Several definitions are necessary prior to discussing Gimpel's technique. With every row r_i of a covering problem associate a Boolean variable (say r_i). The p-function of the covering problem is the associated function of a product-of-sums Boolean expression formed in the following manner. There is a factor $r_{i_1} + r_{i_2} + \dots + r_{i_k}$ in the expression if and only if there is a column covered exactly by rows $r_{i_1}, r_{i_2}, \dots, r_{i_k}$. The significance of the p-function is that a collection of rows $\{r_{i_1}, r_{i_2}, \dots, r_{i_k}\}$ forms a cover of the covering problem if and only if the term $r_{i_1} r_{i_2} \dots r_{i_k}$ is an implicant of the p-function. As an example, $p = r_1 (r_1 + r_2 + r_4) (r_2 + r_3) (r_3 + r_4)$ represents an expression for the p-function of the covering problem defined by Table 2:

r_1	x	x		
r_2		x	x	
r_3			x	x
r_4		x		x

Table 2. Covering Problem

AD-A126 167 ANALYTICAL PROCEDURES FOR TESTABILITY(U) OKLAHOMA UNIV 2/4
NORMAN SCHOOL OF INDUSTRIAL ENGINEERING A A ALY ET AL.
JAN 83 RADC-TR-83-4 F30602-81-C-0012

UNCLASSIFIED F/G 14/2 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

The expression can be reduced to $p = r_1 (r_2 + r_3) (r_3 + r_4) = r_1 r_2 r_4 + r_1 r_3$. These two prime implicants of p correspond to the irredundant covers r_1, r_2, r_4 and r_1, r_3 of the table.

If f is a Boolean function, then the notation $|f|$ denotes the fewest number of literals that appear in any prime implicant of f.

The weight of a column is the number of rows which cover it. The weight of a row is the number of columns which it covers. A covering problem is called plural if every row and every column has weight greater than 1. Note that if a covering problem is not plural it can be reduced by one of the three classical reduction techniques.

A reducing column of a plural covering problem is a column of weight 2 which is not dominated by any other column. If the covering problem is not plural, then it is regarded as not having any reducing columns.

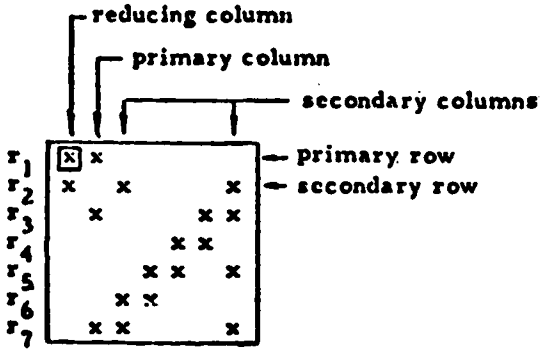
A reducing column of the first kind is a reducing column covered by a row of weight 2. A reducing column of the second kind is a reducing column which is not a reducing column of the first kind.

If a reducing column of a covering problem is covered by rows r_1 and r_2, then the p-function of that covering problem can be written $p = (r_1 + r_2) (r_1 + S) (r_2 + T) P$ where S,T and P are product-of-sums which do not contain r_1 or r_2.

Let C be a covering problem having p as its p-function. Let C_1 be a covering problem whose p-function p_1 is $p_1 = (r_2 + S + T) P$, and C_2 be a covering problem whose p-function p_2 is $p_2 = (S + T) P$. It will be shown how the transformation $C \rightarrow C_1$ can be interpreted as a reduction technique. Moreover, if the reducing column is one of the first kind, then the transformation $C \rightarrow C_2$ can be interpreted as a reduction technique. This reduction technique is now presented in the form of algorithms operating directly on prime implicant tables.

The theorem $|p| = |p_1| + 1$ is stated and proved by Gimpel. A corollary of this is that the transformation $C \rightarrow C_1$ is a reduction technique whose conversion rule is [Select r_2 if S; else r_1]. A second corollary is: let the reducing column of C be a reducing column of the first kind. Then the transformation C → C_2 is a reduction tèchnique. The conversion rule is the same as the conversion rule associated with the reduction technique C → C_1.

Let r_1 and r_2 be rows covering a reducing column of the first kind. Let row r_1 be of weight 2. We call r_1 the primary row and r_2 the secondary row (even if r_2 also has weight 2). We call the entry at the intersection of the primary row and the reducing column the central entry. The primary row covers another column in addition to the reducing column; this column is called the primary column. The columns covered by the secondary row other than the reducing column are called secondary columns. These concepts are illustrated in Table 3:



r_1	☒	x					
r_2	x		x				x
r_3		x				x	x
r_4					x	x	
r_5				x	x		x
r_6			x	x			
r_7		x	x				x

Table 3. Primary and Secondary Rows and Columns

The following algorithm is for a reduction step over a reducing column of the first kind.

a. Given a table, find a reducing table of the first kind and select a central entry.

b. Strike off the reducing column, the primary row, the secondary row, and the primary column.

c. Ignoring the deleted rows in the remaining table, augment each secondary column with the x entries of the primary column.

d. Write the conversion rule [Select r_2 if S_1; else r_1] where r_1 and r_2 are the names, respectively, of the primary and secondary rows, and S_1 is a Boolean expression consisting of the Boolean sum of all the rows that cover the primary column except the primary row.

Tables 4 and 5 illustrate a reduction step over a reducing column of the first kind. The associated conversion rule is [Select r_2 if $(r_3 + r_7)$; else r_1]

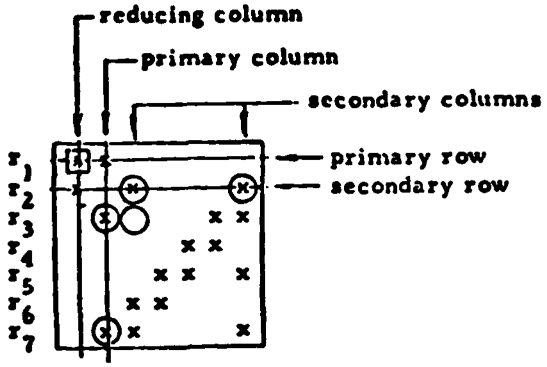


Table 4. Reduction Step

r_3	x			x	x
r_4			x	x	
r_5		x	x		x
r_6	x	x			
r_7	x				x

Table 5. Reduced Table

Table 5 may again be reduced as in Table 6. The associated conversion rule is [Select r_5 if $(r_3 + r_7)$; else r_6].

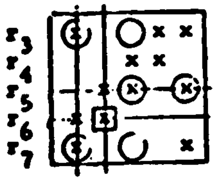


Table 6. Reduction Step

r_3	x	x	x
r_4	x	x	
r_7	x		x

Table 7. Final Table

Table 7 may be reduced by classical techniques and a minimal cover is the single row r_3. Since r_3 is in this cover the second conversion rule is used to add r_5 (and not r_6) to the cover. Similarly the previous rule adds r_2 (and not r_1) to the cover. Thus a minimal cover for the original problem is $\{r_2, r_3, r_5\}$.

To summarize: A reduction step about a reducing column of the first kind reduces the number of rows by two, reduces the number of columns by two, and produces a table having one row less in a minimal cover.

A similar algorithm is presented for a reduction step over a reducing column of the second kind. Gimpel concludes by saying that further reduction techniques are needed to handle other types of problems.

Techniques for finding a minimal cover will also allow a minimum set of tests to be found for the problem of determining tests for built-in-testing. Modifications of Gimpel's work that we would find useful in applying it to BIT problems include an extension to other types of problems, that is, other than those having at least one column covered by exactly two rows, and techniques permitting feasible computation of large problems (Gimpel notes a practical limitation of nine variables).

The relative operating characteristic (ROC) analysis has been borrowed from the general theory of signal detection and has been applied widely in perceptual and cognitive studies in psychology and is used in other fields, including medicine.

Weinstein and Fineberg (1980) discuss the nature and applications of the ROC. ROC curves show the discriminative ability of a test by the position of the full curve in a graph plotting the relation between the true-positive rate (TPR) and the false-positive rate (FPR). The farther upward and to the left the curve lies in Figure 3, the better is the test, as shown.

The ROC graph also distinguishes that inherent discriminative ability of the test from the user's choice of a positivity criterion, which is indicated by any particular point on the curve.

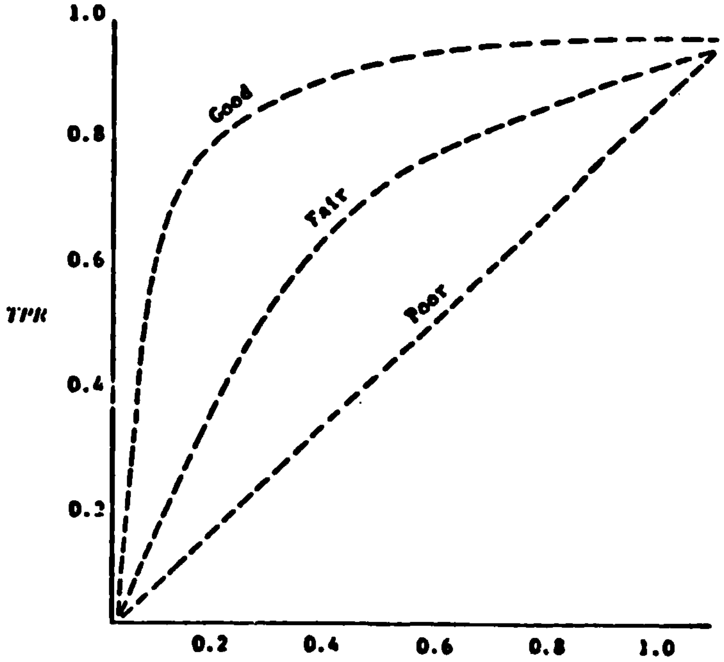


Figure 3. A Comparison of Tests Using Their ROC Curves

They also explain the use of ROC curves in ranking tests. Imagine that there has been collected from the literature reports of four different diagnostic tests -- B, C, D, and E -- for the same condition and that it is proposed to compare them with the present standard test, A. The reports include information from which we can calculate the true-positive and false-positive rates (TPR and FPR) at a specified cutoff point, but, as is almost always the case, they do not include sufficient information to construct the full ROC curves.

Begin by constructing a coordinate system (see Figure 4), with its origin at the pair of values for the TPR and the FPR that symbolize the performance of test A in the ROC plane. Test C falls in the right lower quadrant of this new coordinate system; from what is already known of the shape of ROC curves, the curve indicating the performance of test C will lie below and to the right of the ROC curve passing through point A. Assuming other things, such as costs and risks, to be the same in both tests, it may safely be concluded, then, that test A is superior to test C. Similarly, test B, which is indicated by the ROC curve that passes through point B, must be better than test A, which is represented by the ROC curve that passes through point A.

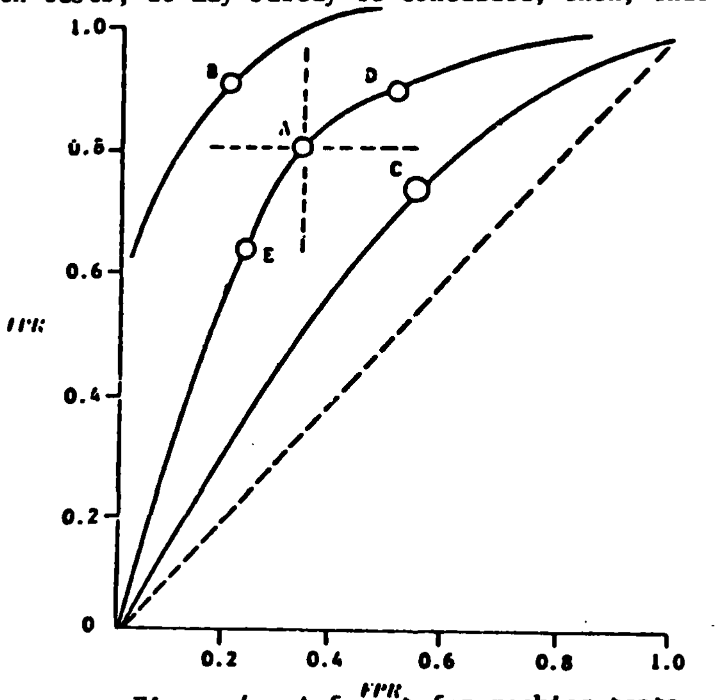


Figure 4. A format for ranking tests

The relative merits of tests D and E are less clear. Given what is already known of the general shape of ROC curves and this limited information about tests D and E, it is possible that points E, A, and D lie on the same ROC curve and that the differences in the values of the TPR and the FPR result only from the particular choices of the cutoff points used in the three reports. From the standpoint of an analysis based on the ROC curve, points E, A, and D could belong to the same test, with each point representing a different trade-off between test sensitivity and specificity. In contrast to points B and C, which the ROC analysis unambiguously demonstrates to be superior and inferior, respectively, to A, the approach by itself does not permit conclusions as to the relative merits of operating at point E, A, or D.

Swets et al. (1979) use this technique to do a comparative study of two radiologic techniques. From it they are able to evaluate the relative performance of the tests.

In the problem of built-in-testing this method would be applicable in the case when tests may be considered to be less than 100% reliable. Our term for a false-positive result is a false alarm. Several tests of a given unit may be compared based on their false alarm rates.

Earlier, the attempt of Sheskin (1979) to solve the partitioning problem was discussed. This problem involves deciding which LRUs should be grouped together as a unit for testing purposes. A heuristic approach is suggested in MIL-STD-1591 but its solution is dependent on the starting point. Since Sheskin's approach fails to yield an optimum solution a modification to provide optimality is needed. This modification must allow the solution to be computationally feasible and yet provide an overall optimum partitioning problem.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

In this study, a comprehensive literature review has been performed to uncover any material pertinent to the testability area. In the research ef:ort, the testability area encompasses both fault detection and isolation for a malfunctioned system. The main thrust of the work was to identify basic analytical tools to be utilized in checking the reliability of testing systems. Several other tasks have been addressed and analyzed mainly;

i. Discussion of concepts, terms and models used in the testability area. From the literature survey it was discovered that several definitions of terms, parameters and measures are ambiguous and very misleading if used directly in measuring the reliability of the system.

ii. The problem of developing multi-parameter testability evaluation models has been tackled. However, due to the complexity of the problem few examples were presented. In specific, the combination of fault detection probability along with the false alarm probability resulted in a more ambiguous figure of merit and it was shown, analytically, the type of error which could be incurred in the system.

iii. Design analysis tools for each level of maintenance (organization, shop, and depot) have been developed. Some constructed cost models proved to be useful in designing an optimal configuration of testers at each level such as BIT and TE.

iv. From the open and closed literature a complete annotated bibliography was developed. Technical critique of current state-of-the-art testability technology showed the technical feasibility, limitations, and practicality of existing procedures.

v. Other disciplines address problems similar to the testability problem in its design, evaluation, and optimization stages. Some of the models and techniques were easily adaptable to the system under study with minor modification and others required major modification. Both types have been analyzed and the problem of adaptations was discussed.

5.2 Recommendations

From the above study, the development of comprehensive baseline tools and procedures are far from completion. The following research efforts are recommended for a future work;

i. Expand the critique of parameters and measures to cover most of the feasible combinations between them. Analytical models, using different logic circuits, should be constructed to support the baseline tools and parameters.

ii. Develop a multimaintenance tier testability evaluation model(s) which will contain all levels of maintainability parameters at the organization, shop, and depot. This model(s) will provide more information about both the cost and reliability of the system.

iii. Development of optimization procedures to the above model(s). This will yield an optimum system testability and will also provide a good tool to identify any individual testability parameters and will handle any changes of dynamic nature.

iv. Those models and techniques identified above which require major modification to be utilized in the testability area must be studied, analyzed and modified.

v. Testing any of the above models and techniques with real data. This will require coding all algorithms in a computer language and testing their applicabilities for use in electronic equipment and systems.

REFERENCES

Abraham, J.A. and Thatte, S.M., "Fault Coverage of Test Programs for a Microprocessor," IEEE Test Conference (1979), pp 18-22.

Agarwal, Vinod K. and Masson, Gerald M., "A Functional Approach to Test Set Coverage in Tree Networks", **IEEE Transactions on Computers**, Vol. C-27 (1979), pp 50-52.

Akers, Sheldon B., Jr., "Fault Diagnosis as a Graph Coloring Problem", **IEEE Transactions on Computers**, Vol C-23 (1974), pp 706-713.

Allan, F.J.; Kameda, T,; and Toida, S., "An Approach to the Diagnosability Analysis of a System", **IEEE Transactions on Computers**, Vol C-24 (1975), pp 1040-1042.

Allen, David J. and Rao, M.S. Madhava, "New Algorithms for the Synthesis and Analysis of Fault Trees", **Industrial Engineering Chemical Fundamental**, Vol 19 (1980), pp 79-85.

Aly, A.A., "Optimal Design of Built-in-Test Diagnostic Systems," A report submitted to AFOSR (1979).

Aly, A.A., "Optimum Testing Procedures for System Diagnosis and Fault Isolation," University of Oklahoma, School of Industrial Engineering, Technical Report No. 80-10, Norman, OK (1980)

Aly, A.A., and Elsayedaly, E.A., "An Efficient Algorithm for Optimal Design of Diagnostics", University of Oklahoma School of Industrial Engineering, Technical Report No. 81-3, Norman, OK (1981).

Armstrong, D.B., "On Finding a Nearly Minimal Set of Fault Detection Tests for Combinational Logic Nets," **IEEE Transactions on Computers**, Vol C-25 (1976), pp 585-593.

Barsi, Ferruccio; Grandoni, Fabrizio; and Maestrini, Piero, "A Theory of Diagnosability of Digital Systems," **IEEE Transactions on Computers**, Vol C-25 (1976), pp 585-593.

Ben-dov, Y., "Optimal Testing Procedures for Coherent Systems," AD A057952, (1977).

Bogard, D.R. et al., "Operation and Support Cost Characteristics of Testers and Test Subsystems", RADC-TR-79-334, Final Technical Report (1980).

Breuer, Melvin A.; Chang, Shih-Jeh; and Su, Stephen Y..H., "Identification of Multiple Stuck-Type Faults in Combinational Networks", **IEEE Transactions on Computers**, Vol C-25 (1976), pp 44-54.

Brulé, J.D.; Johnson, R.A. and Kletsky, E.J., "Diagnosis of Equipment Failures," **IRE Transactions on Reliability and Quality Control**, Vol. RQC-9 (1960), pp 23-34.

Butterworth, T., "Some Reliability Fault Testing Models," **Operations Research**, Vol 20, (1972).

Carroll, B.D. and Smith, E.W., "A Bibliography of Fault Tolerant Computing," AD:739522, (1972).

Chang, Herbert Y., "An Algorithm for Selecting an Optimum Set of Diagnostic Tests", **IEEE Transactions on Electronic Computers**, Vol EC-14 (1965), pp 706-711.

Chang, Herbert Y., "Figures of Merit for the Diagnostic of a D[illegible]al System", **IEEE Transactions on Reliability**, Vol R-17 (1968), pp 147-153.

Clegg, F.W., "Use of SPOOF's in the Analysis of Faulty Lc[illegible] Networks," **IEEE Transactions on Computers**, Vol C-22, pp 229-234 (1973).

Cohn, M. and Ott, G., "Design of Adaptive Procedures for Faul[illegible]ection and Isolation", **IEEE Transactions on Reliability**, Vol R-20, (1971), pp 7-10.

Conley, G., "Digital System Diagnostics - Design/Evaluations", Proceedings of the Annual Reliability and Maintainability Symposium (1980).

Consolla, W.M. and Danner, F.G., An Objective Printed Circuit Board Design Guide and Rating System, RADC-TR-79-327, (1980).

Cox, Glenn W. and Carroll, B.D., "Reliability Modeling and Analysis of Fault-Tolerant Memories", **IEEE Transactions on Reliability**, Vol R-27 (1978), pp 49-53.

Deo, Narsingh, The Self-Diagnosability of a Computer," **IEEE Transactions on Electronic Computers**, Vol EC-15 (1966), p 799.

Du, Min-Wen, "A Way to Find a Lower Bound for the Minimal Solution of the Covering Problem", **IEEE Transactions on Computers**, Vol C-21 (1972), pp 317-318.

Fantauzzi, G., and Marsella, A., "Multiple Fault Detection and Location in Fan-Out Free Combinational Circuits," **IEEE Transactions on Computers**, Vol C-23, pp 48-54 (1974).

Firstman, S., and Gluss, B., "Optimum Search Routines for Automatic Fault Location," **Operations Research**, Vol 8 (1960).

Freedy, Amos and Lucaccini, Luigi F., "Adaptive Computer Training System (ACTS) for Fault Diagnosis in Maintenance Tasks", **NATO Symposium on Human Detection and Diagnosis of System Failures** (1980), pp. 637-658,

Friedman, Arthur D., "Comment on 'A Method for the Selection of Prime Implicants'", **IEEE Transactions on Electronic Computers**, Vol EC-16 (1967), pp 221-222.

Friedman, A.D. and Menon, P.R., **Fault Detection in Digital Circuits**, Prentice-Hall, Englewood Cliffs, New Jersey (1971).

Fujiwara, Hideo and Kinoshita, Kozo, "Connection Assignments for Probabilistically Diagnosable Systems", **IEEE Transactions on Computers**, Vol C-27 (1978 a), pp 280-283.

Fujiwara, Hideo and Kinoshita, Koza, "On the Computational Complexity of System Diagnosis", **IEEE Transactions on Computers**, Vol C-27 (1978 b), pp 881-885.

Gaertner, W.W., "Development of BIT Equipment for Tactical FM Radios", Army Electronics Command, AD: A005277.

Gimpel, James F., "A Reduction Technique for Prime Implicant Tables, **IEEE Transactions on Electronic Computers**, Vol EC-14 (1965), pp 535-541.

Gleason, D., "A Measure of BIT/ETE Effectiveness," A working paper, USAF, RADC/RBET, Griffis AFB, Rome, New York (1981).

Gluss, B., "An Optimum Policy for Detecting a Fault in a Complex System," **Operations Research**, Vol 7 (1959).

Goel, Prabhaker, "An Implicit Enumeration Algorithm to Generate Tests for Combinational Logic Circuits", **IEEE Transactions on Computers**, Vol C-30 (1981), pp 215-222.

Hadlock, Frank, "On Finding a Minimal Set of Diagnostic Tests", **IEEE Transactions on Electronic Computers**, Vol EC-16 (1967), pp 674-675.

Hakimi, S.L. and Amin, A.T., "Characterization of Connection Assignment of Diagnosable Systems", **IEEE Transactions on Computers**, Vol C-23 (1974), pp 86-88.

Hakimi, S. Louis, "Fault Analysis in Digital Systems - A Graph Theoretic Approach", **Rational Fault Analysis**, (1973).

Halpern, Jonathan, "A Sequential Testing Procedure for a System's State Identification", **IEEE Transactions on Reliability**, Vol R-23 (1974), pp 267-272

Happ, W.W. and Sarkisian, E., "Combinatorial Techniques for Fault Identification in Multi-Terminal Networks", Annual Symposium on Reliability (1968), pp 477-485.

Hartwell, W.T.; Hoffner, C.W.; and Toy, W.N., "A Fault Tolerant Memory for Duplex Systems," **IEEE Transactions on Reliability**,Vol R-27 (1978), pp 134-138.

Hayes, John P., On Realization of Boolean Functions Requiring a Minimal or Near-Minimal Number of Tests," **IEEE Transactions on Computers**, Vol C-20 (1971), pp 1506-1513.

Hayes, John P., "Transition Count Testing of Combinational Logic Circuits," **IEEE Transactions** on **Computers**, Vol C-25 (1976), pp 613-620.

Hecht, Herbert, "Fault-Tolerant Software," **IEEE Transactions on Reliability**,Vol R-28 (1979), pp 227-232.

Heckelman, R.W., et al., "Self Diagnosing Design Techniques", General Electric, Publication Number AFAL-TR-78-183 (1981).

Himmelblau, D.M., **Fault Detection and Diagnosis in Chemical and Petrochemical Processes** (1978).

Horkovich, James A., "Automatic Fault Detection/Fault Isolation Systems: Requirements and Testing", AFTEC Logistics Assessment Procedures Division, Kirtland AFB (1981).

Hornbuckle, Gary D. and Spann, Richard N., "Diagnosis of Single-Gate Failures in Combinational Circuits", **IEEE Transactions on Computers**, Vol C-18 (1969), pp 216-220.

Johnson, R.A., "An Information Theory Approach to Diagnosis", 6th Symposium on Reliability and Quality Control (1960), pp 102-109.

Johnson, R.A., et al. "Diagnosis of Equipment Failures", Syracuse University Research Technical report (AD-213876) (1959).

Johnson, Richard A. and Brulé, John D., **Diagnosis of Equipment Failures**, RADC-TR-60-67A (1960).

Karunanithi, S. and Friedman, Arthur D., "Analysis of Digital Systems Using a New Measure of System Diagnosis," **IEEE Transactions on Computers**, Vol C-28 (1979), pp 121-133.

Kautz, William H., "Fault Testing and Diagnosis in Combinational Digital Circuits", **IEEE Transactions on Computers**, Vol C-17 (1968), pp 352-366.

Kime, Charles R., "An Analysis Model for Digital System Diagnosis", **IEEE Transactions on Computers**, Vol C-19 (1970), pp 1063-1073.

Kime, Charles R., "Fault Tolerant Computing: An Introduction and a Perspective", **IEEE Transactions on Computers**, Vol C-24 (1975), pp 457-460.

Kletsky, E.J., "Diagnosis of Equipment Failures", RADC-TR-60-67B, Final technical Report, Part 2/2, (1960).

Kletsky, E.J., "An Application of the Information Theory Approach to Failure Diagnosis," **IRE Transactions on Reliability and Quality Control**, Vol RQC-9, (1960), pp 29-39.

Kohavi, Zvi and Berger, Israel, "Fault Diagnosis in Combinational Tree Networks," **IEEE Transactions on Computers**, Vol C-24 (1975), pp 1161-1167.

Koren, Israel and Kohavi, Zvi, "Sequential Fault Diagnosis in Combinational Networks," **IEEE Transactions on Computers**, Vol C-26 (1977), pp 334-342.

Levy, Girard W., et al., "Final Report on Improved Maintenance Procedures for Inertial Guidance Systems", PRAM Program Office, AFSC, Aeronautical Systems Division: Wright-Patterson AFB (1976).

Liguori, Fred, "Introduction to Current Computer Aids to Digital Test Design for Automated Test Equipment," **SETE Workshop Proceedings** (1974).

Linden, V.L., "Diagnostic Development - A New Prospective", **ATE Newsletter** (1981).

Luccio, F., "Reduction of the Number of Columns in Flow Table Minimization", **IEEE Transactions on Electronic Computers**, Vol EC--15 (1966), pp 803-805.

Maheshwari, Shachindra N. and Hakimi, S. Louis, "On Models for Diagnosable Systems and Probabilistic Fault Diagnosis", **IEEE Transactions on Computers**, Vol C-23 (1976), pp 228-226.

Malek, Miroslav and Liu, Kuen Y., "Graph Theory Models in Fault Diagnosis and Fault Tolerance", **Design Automation and Fault-Tolerant Computing**, Vol 3 (1980), pp 155-169.

Mandelbaum, David, "A Measure of Efficiency of Diagnostic Tests Upon Sequential Logic", **IEEE Transactions on Electronic Computers**, Vol EC-13 (1964), p 630.

Mayeda, Wataru and Ramamoorthy, C.V., "Distinguishability Criteria in Oriented Graphs and Their Application to Computer Diagnosis-I", **IEEE Transactions on Circuit Theory**, Vol CT-16 (1969), pp 448-454.

McCluskey, E.J., "Testing and Diagnosis of Logic", EURO IFIP (1979), pp 735-738.

McPherson, John A. and Kime, Charles R., "A Two-Level Diagnostic Model for Digital Systems," **IEEE Transactions on Computers**, Vol C-27 (1979), pp 16-27.

Meyer, Gerald G.L. and Masson, Gerald M., "An Efficient Fault Diagnosis Algorithm for Symmetric Multiple Processor Architectures," **IEEE Transactions on Computers**, Vol C-27 (1978), pp 1059-1063.

Meyer, John F. and Rault, Jean-Claude, "Fault-Tolerant Computing: An Introduction", **IEEE Transactions on Computers**, Vol C-25 (1976), pp 553-556.

Military Standards On-Aircraft, Fault Diagnosis, Sub-Systems, Analysis/Synthesis Of, MIL-STD-1519 (1977).

Nakano, Hideo and Nakanishi, Yoshiro, "Internal Test Terminals for Systems Diagnosis," **Electronics and Communications in Japan**, Vol 54-C (1971 a).

Nakano, Hideo and Nakanishi, Yoshiro, "A Procedure of Determining Test Terminals for System Diagnosis", **Systems*Computers*Controls**, Vol 2 (1971 b), pp 58-63.

Nakano, Hideo and Nakanishi, Yoshiro, "Necessary and Sufficient Conditions for 1-Distinguishablility in System Diagnosis", **Systems*Computers*Controls**, Vol 3 (1972), pp 52-57.

Nakano, Hideo and Nakanishi, Yoshiro, "Graph Representation and Diagnosis for Multiunit Faults", **IEEE Transactions on Reliability**, Vol R-23 (1974), pp 320-325.

Pau, L.F., "Application of Pattern Recognition to Failure Analysis and Diagnosis," **Human Detection and Diagnosis of System Failures** (1980), pp 389-409.

Pieper, W.J., et al., "Computer Generated Troubleshooting Trees: Application and Tryout," AD 004634.

Pliska, T.F., Jew, F.L., Angus, J.E., "BIT/External Test Figures of Merit and Demonstration Techniques." RADC-TR-79-309, Rome, N.Y., (1979).

Poage, J.F., "Derivation of Optimum Tests to Detect Faults in Combinational Circuits," **Mathematical Theory of Automata**, Brooklyn, New York, Polytechnic Press, pp 483-528 (1963).

Powell, Theo J., "A Procedure for Selecting Diagnostic Tests", **IEEE Transactions on Computers**, Vol C-18 (1969), pp 168-175.

Preparata, Franco P.; Metze, Gernot; and Chien, Robert T., "On the Connection Assignment Problem of Diagnosable Systems," **IEEE Transactions on Electronic Computers**, Vol EC-16 (1967), pp 848-854.

Preparata, Franco P., "An Estimate of the Length of Diagnostic Tests", **IEEE Transactions on Reliability**, Vol R-18 (1969), pp 131-136.

Ramamoorthy, C.V., and Mayeda, W., "Computer Diagnosis Using the Blocking Gate Approach," **IEEE Transactions on Computers**, Vol C-20 (1971), pp 1294-1299.

Rao, C.V.S. and Biswas, Nripendra N., "Minimization of Incomplexity Specified Sequential Machines," **IEEE Transactions on Computers**, Vol C-24 (1975), pp 1089-1100.

Risse, Thomas, "On the Structure of Self-Diagnosing System," **Methods of Operations Research**, Vol 43 (1981), pp 433-441.

Robinson, Stanley U. III and House, Robert W., "Gimpel's Reduction Technique Extended to the Covering Problem with Costs", **IEEE Transactions on Electronic Computers**, Vol EC-16 (1967), pp 509-514.

Rosenthal, Arnon, "Decomposition Methods for Fault Tree Analysis," **IEEE Transactions of Reliability**, Vol R-29 (1980), pp 136-138.

Roth, J.P., Bouricius, W.G. and Schneider, P.R., "Programmed Algorithms to Compute Tests to Detect and Distinguish Between Failures in Logic Circuits," **IEEE Transactions on Electronic Computers**, Vol EC-16, pp 567-580 (1967).

Russell, Jeffrey D. and Kime, Charles R., "System Fault Diagnosis: Masking, Exposure, and Diagnosability Without Repair," **IEEE Transactions on Computers**, Vol C-24 (1975), pp 1155-1161.

Scola, P.J., "Tolts, Total On-Line Testing System" Index Serial Number 1084, pp 306-312.

Sellers, F.F., Hsiao, M.Y. and Bearnson, L.W., "Analyzing Errors with the Boolean Difference," **IEEE Transactions on Electronic Computers**, Vol. C-17, pp 678-683 (1968).

Seshu, Sundaram, **Self-Repairing Machines**, RADC-TR-61-91B (1961).

Seshu, Sundaram, "On an Improved Diagnosis Program", **IEEE Transactions on Electronic Computers**, Vol EC-14 (1965), pp 76-79.

Seshu, S. and Freeman, D.N., "The Diagnosis of Asynchronous Sequential Switching Systems", **IRE Transactions on Electronic Computers**, Vol EC-11 (1962), pp 459-465.

Sheskin, T.J., "Design of System Diagnostic and Fault Isolation Procedures" USAF/ ASEE Summer Faculty Research Program, Vol 2, AFOSR-TR-78-0349 (1977), AD-A051514.

Sheskin, T.J., "Sequencing of Diagnostic Tests for Fault Isolation by Dynamic Programming," **IEEE Transactions on Reliability**, Vol R-27 (1978), pp 353-358.

Sheskin, T.J., "Fault Isolation for Modular Electronic Equipment", Proceedings of the Annual Reliability and Maintainability Symposium, (1979).

Sheskin, T.J., "Specifications of Built-In-Tests for Modular Equipment," AFOSR USAF Grant, AFOSR-78-3496.

Slagle, James R.; Chang, Chin-Liang; and Lee, Richard C.T., "A New Algorithm for Generating Prime Implicants", **IEEE Transactions on Computers**, Vol C-19 (1970), pp 304-310.

Susskind, Alfred K., "Diagnostics for Logic Networks", **IEEE Spectrum** (1973), pp 40-47.

Swets, John A. et al., "Assessment of Diagnostic Technologies", **Science**, Vol 205 (1979), pp 753-759.

Takami, I. et al., "Optimal Allocation of Fault Detectors", **IEEE Transactions on Reliability**, Vol R-27, No. 5 (1978).

Tasar, V., "Analysis of Fault Detection Coverage of a Self-Test Software Program," D. Eng. Dissertation, University of Detroit, Detroit, Michigan (1977).

Tasar, Vehbi and Ohlef, Henry L., "A Method for Determining the Statistically Weighted Percent Fault Detection Coverage of a Self-Test Program", Proceedings of the 1979 Annual Reliability and Maintainability Symposium, pp 39-43.

Toida, S., "System Diagnosis and Redundant Tests," **IEEE Transactions on Computers**, Vol C-25 (1976), pp 1167-1170.

Tuttle, D.E. and Loveless, R., "Built-In-Test and External Tester Reliability Characteristics," RADC-TR-80-32, Rome, New York (1980).

Weinstein, Milton and Fineberg, Harvey, **Clinical Decision Analysis** (1980).

Weisberg, Stuart A. and Schmidt, John A., "Computer Technique for Estimating System Reliability", Annual Symposium on Reliability (1966), pp 87-97.

Weiss, C. Dennis, "Bounds on the Length of Terminal Stuck-Fault Tests", **IEEE Transactions on Computers** (1972), pp 305-309.

Williams, Michael J.V. and Angell, James B., "Enhancing Testability of Large-Scale Integrated Circuits via Test Points and Additional Logic," **IEEE Transactions on Computers**, Vol C-22 (1973), pp 46-60.

Winter, B.B, "Optimal Diagnostic Procedures", **IRE Transactions on Reliability and Quality Control**, Vol RQC-9 (1960).

Vink, H.A.; Dolder, B. van der; and Al, J., "Reduction of CC-Tables Using Multiple Implication", **IEEE Transactions on Computers**, Vol C-27 (1978), pp 961-966.

"A Sequential Approach to Heart-Beat Internal Classifications", AD: A018516.

"A System of Computer Aided Diagnosis with Blood Serum Chemistry Tests and Bayesian Statistics", AD: 786284.

APPPENDIX

ANNOTATED BIBLIOGRAPHY

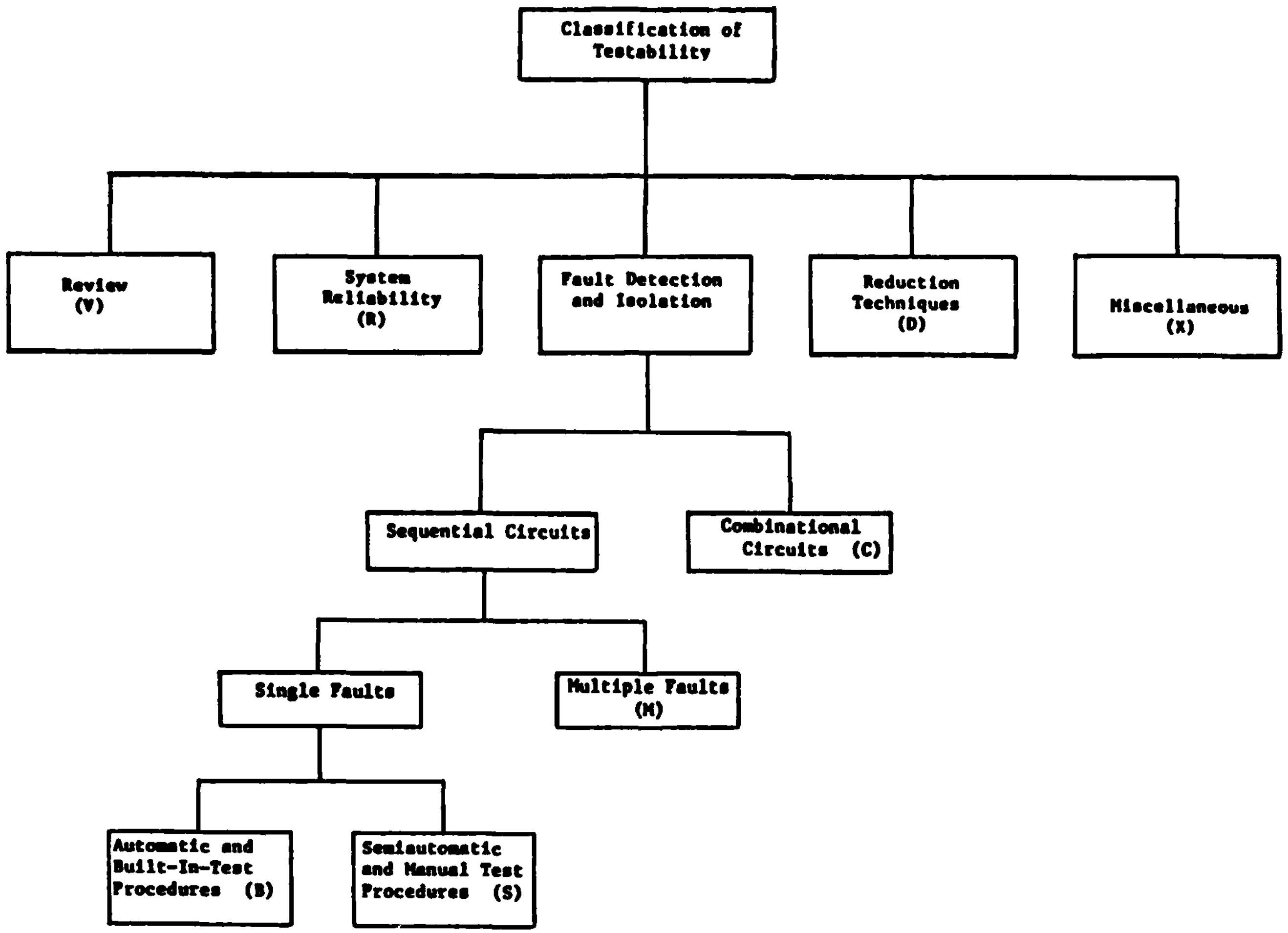

Classification of Testability
Review (V)
System Reliability (R)
Fault Detection and Isolation
Reduction Techniques (D)
Miscellaneous (X)
Sequential Circuits
Combinational Circuits (C)
Single Faults
Multiple Faults (M)
Automatic and Built-In-Test Procedures (B)
Semiautomatic and Manual Test Procedures (S)

Figure 5. Classification of Testability

B - AUTOMATIC AND BUILT-IN-TESTS

B-1. Firstman, S., and Gluss,B., "Optimum Search Routines for Automatic Fault Location," Operations Research, Vol. 8 (1960).

B-2. Gleason, D., "A Measure of BIT/ATE Effectiveness," USAF, RADC/RBET, Griffis AFB, Rome, New York.

B-3. Johnson, R.A. et al., "Diagnosis of Equipment Failures," Syracuse University Research Technical Report (AD-213876) (1959).

B-4. Pieper, W.J. et al., "Computer Generated Troubleshooting Trees: Application and Tryout," AD-004634.

B-5. Pliska, T.F. Jew, F.L. and Angus, J.E., "BIT/External-Test Figures of Merit and Demonstration Techniques," RADC-TR-79-309, Rome, New York (1979).

B-6. Sheskin, T.J., "Design of System Diagnostic and Fault Isolation Procedures," 1977 USAF/ASEE Summer Faculty Research Program, Vol. 2, AFOSR-TR-78-0349, AD-A051514.

B-7. Sheskin, T.J., "Specification of Built-in-Tests for Modular Equipment," USAF Grant, AFOSR-78-3496.

B-8. Sheskin, T.J., "Partitioning of Modular Equipment for Fault Isolation," Microelectronics and Reliability, Vol 17, Pergamon Press Ltd. (1978).

B-9. Sheskin, T.J., "Sequencing of Diagnostic Tests for Fault Isolation by Dynamic Programming," IEEE Transactions on Reliability, Vol. R-27 (1978).

B-10. Sheskin, T.J., "Fault Isolation for Modular Electronic Equipment," (1979). Proceedings of the Annual Reliability and Maintainability Symposium.

B-11. Tasar, V. and Ohlef, H.L., "A Method for Determining the Statistically Weighted Percent Fault Detection Coverage of a Self-Test Program," (1979). Proceedings of the Annual Reliability and Maintainability Symposium.

B-12. Tuttle, D.E. and Loveless,R., "Built-In-Test and External Tester Reliability Characteristics," RADC-TR-80-32, Rome, New York (1980).

B-13. Takimi, I. et al., "Optimal Allocation of Fault Detectors," IEEE Transactions on Reliability, Vol. R-27 (1978).

B-14. Linden, V.L., "Diagnostic Development - A New Prospective," ATE Newsletter (1981).

B-15. Gaertner, W.W.,"Development of BIT Equipment for Tactical FM Radios," Army Electronics Command, AD-A005277.

B-16. Horkovich, James A., "Automatic FD/FI Systems: Requirements and Testing," AFTEC Logistics Assessment Procedures Division, Kirtland AFB.

B-17. "JLC Panel on Automatic Testing - Subtask Description," (1979).

B-18. "Study Plan for JLC Panel on Automatic Testing," (1978).

B-19. "Military Standards On-Aircraft, Fault Diagnosis, Sub-Systems, Analysis/Synthesis Of" Department of Defense, MIL-STD-1591 (1977).

B-20. Heckelman, R.W. et al., "Self Diagnosing Techniques," Electronics Laboratory. General Electric Publication Number AFAL-TR-78-183, Syracuse, New York (1981).

B-1

TITLE: Optimum Search Routines For Automatic Fault Location

AUTHOR: Firstman, S., and Gluss, B.

JOURNAL: Operations Research, Vol. 8, pp. 512-523, 1960

SCOPE: Fault Test models using BIT and secondary isolation.

PROBLEM DEFINITION: A system consists of N modules. Each module contains a number of elements. It is required to find the optimal search tests to find first the faulty module, and secondly the faulty component in that module using an automatically sequenced testing machine.

ASSUMPTIONS:

1) Only one fault exits.
2) The module is not retested until after all components have been tested.

SOLUTION APPROACH: Mathematical Models

CONCLUSIONS:

1) A model is derived to find a feasible test sequence to locate the faulty module then the faulty component in it. (The search sequence derived by this model is not necessarily optimal).

2) The probabilities of faults lying in respective modules are computed from element reliability data by manipulation of their failure rates.

B-2

TITLE: A Measure of BIT/ATE Effectiveness

AUTHOR: Gleason, Daniel

JOURNAL: USAF, RADC/RBET, Griffis AFB, Rome, NY

SCOPE: Systems with BIT/ATE

PROBLEM DEFINITION: To make use of BIT/ATE specification and maintenance policy factors in order to evaluate the overall effectiveness of the designated BIT/ATE system.

CONSTRAINTS/ASSUMPTIONS: One failure exists at the time that the unit is undergoing test. Fault detection capability of ATE/BIT is equal in all diagnostic groups. Probability of misassignment is equal for all diagnostic groups.

SOLUTION APPROACH: A BIT/ATE is modelled with certain fault detection and isolation capability specified. The four BIT/ATE specifications are:

1. Fault detection capability P (FD)
2. Average ambiguity level $\bar{x}$.
3. Misassignment factor P(MA)
4. False alarm factor FAR and the maintenance policy Removal Rate RR_i are used in evaluating the effectiveness of the BIT/ATE system.

BIT/ATE diagnostic event tree is shown, summarizing all the events that can occur.
Next sensitivity analysis is carried out on the expected number of removals (ENR).

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: BIT/ATE specifications applicable to avionics are presented. Compilations of sensitivity analysis evaluation for i) iterative removal policy and ii) group removal policy are tabulated.

The number of removals that a prime system experiences per prime system failure is a measure of how effectively the associated test equipment is performing its designated job of Fault Selection/Isolation. The figures provide an engineer capability to assess numerous logistic performance parameters, and relate these factors to overall life cycle cost.

B-3

TITLE: Diagnosis of Equipment Failures

AUTHOR: Johnson, R.A., Kletsky, E., and Brulé, J.

JOURNAL: Syracuse University Research Technical Report (AD-213876), 1959.

SCOPE: Fault Diagnosis Using Automatic Sequential Tests

PROBLEM DEFINITION: An equipment consists of N functional elements. The equipment has malfunctioned due to failure of one and only one element. It is required to find a sequential test procedure to locate the malfunctioned element with minimum cost.

ASSUMPTIONS:

1. Multiple failure is neglected.
2. The results of tests are unequivocal.

SOLUTION APPROACH: The information gain theory is used to provide a figure of merit with which it is possible to construct an efficient testing procedure. If the initial status of the equipment is specified by the a priori probabilities of failure of the individual LRUs, then in any complete testing procedure this initial ambiguity is reduced until the faulty unit is identified at the final state and the ambiguity of this state becomes zero. Therefore, minimizing the average cost of testing procedures is equivalent to minimizing the average cost per unit ambiguity removed for the procedure.

COMPUTATIONAL EXPERIENCE: Solved examples.

CONCLUSIONS:

1. General models for the diagnosis of equipment failures are presented.
2. The information theory approach provides a systema way of finding a good - but not optimal - testing procedure.

B-4

TITLE: Computer Generated Troubleshooting Trees: Application and Tryout

AUTHOR: Pieper, W.J. et al.

JOURNAL: AD: A004634

SCOPE: Fault diagnosis by Automatic Tests

PROBLEM DEFINITION: Developing an effective technology for computer generation of troubleshooting trees which helps the development of improved maintenance documentation. Also aids in generating and validating troubleshooting trees for finding faults in a test system.

ASSUMPTIONS:

1. The trees must be accurate.
2. They must be exhaustive in terms of finding the faulty system component regardless of the malfunction indication.
3. The troubleshooting logic trees must be efficient.

SOLUTION APPROACH: Computer Program

COMPUTATIONAL EXPERIENCE: The proposed computer program was transliterated into FORTRAN IV language. Then it was applied to the AN/APN-147 doppler radar system. The program could not handle some of the circuits in the test system.

CONCLUSIONS:

1. Computer generation of troubleshooting trees is feasible.
2. The proposed program worked efficiently.
3. Computer processing is fast and works well with systems up to 300 components.
4. Problems are encountered only when a large number of systems states and large complex feedbackloops exist simultaneously.

B-5

TITLE: BIT/External Test-Figures of Merit and Demonstration Techniques

AUTHOR: Pliska, T.F. et al.

JOURNAL: Final Technical Report, RADC-TR-79-309, Dec. 79

SCOPE: Equipment with BIT/ETE environment

PROBLEM DEFINITION: To identify and define figures of merit (FOM) to express the adequacy of BIT/ETE and, to develop methods to analyze and demonstrate the defined FOM.

SOLUTION APPROACH: Categorized into

a) Data Collection: Surveying the existing FOMs.
b) FOM Evaluation: A weighted rating evaluation of the suitability of the defined FOM as design specification.
c) Analysis/demonstration techniques development.
d) FOM specification guidelines.

A summary of BIT/ETE requirements specified by military standards and certain specific systems are included. The objectives of the BIT/ETE are categorized along with the respective FOMs identified. The terms and definitions associated with BIT/ETE are defined in detail.

Factors such as ambiguity, translatability, trackability, demonstratability, applicability and uniqueness are used in determining the suitability of BIT/ETE FOMs with appropriate weights associated with them.

Final evaluation scores are tabulated.

CONCLUSIONS: BIT/ETE FOMs currently used do not cover all aspects of BIT/ ETE capability and are ambiguous and inconsistent.

Necessary tools required to integrate the defined BIT/ETE FOM into standard maintainability programs are discussed.

Further study in the area of false alarms, automated circuit analysis and cost-trade offs are suggested.

B-6

TITLE: Design of System Diagnostic and Fault Isolation Procedures

AUTHOR: Sheskin, T.J.

JOURNAL: 1977 USAF/ASEE Summer Faculty Research Program, Vol. 2, AFOSR-TR-78-0349, AD-A051514

SCOPE: Fault diagnosis using BIT

PROBLEM DEFINITION:

1. Determine the sequence of diagnostic tests to be executed to isolate the failed unit from the group of modules identified by the BIT whenever the equipment malfunctions.
2. Partition the equipment into near optimum subgroups of modules, such that the average cost of isolating the faulty unit is minimized.

ASSUMPTIONS: Multiple failure is neglected

SOLUTION APPROACH: Dynamic Programming

COMPUTATIONAL RESULT: Solved examples

CONCLUSIONS:

1. Probabilistic dynamic programming has been proposed as a new approach which is guaranteed to generate a minimum cost sequence of BIT primary diagnostic tests.
2. A new effective heuristic procedure for partitioning the equipment into subgroups of LRUs to be called out by the primary diagnostic utilizes deterministic dynamic programming to derive weights for the subgroups and binary linear programming to produce a low cost partition based on these weights.

B-7

TITLE: Specification of Built-In-Tests for Modular Equipment

AUTHOR: Sheskin, T.J.

JOURNAL: AFOSR, USAF Grant AFOSR-78-3496

SCOPE: Fault Diagnosis Using BIT

PROBLEM DEFINITION:

1) An equipment consisting of N LRUs has been partitioned into k mutually exclusive groups of modules. It is required to identify the group of modules which contains a single failed element.
2) Partition the equipment into mutually exclusive groups of modules and specify a set of BIT Procedures which will diagnose this partition after the equipment has failed.

ASSUMPTIONS: Multiple failure is neglected

SOLUTION APPROACH: Dynamic Programming

COMPUTATIONAL RESULTS: Solved examples

CONCLUSIONS: A hybrid dynamic programming procedure is derived for determining both the optimum partition of modular electronic equipment into mutually exclusive groups of LRUs and the minimum cost set of BIT which acts on this partition.

B-8

TITLE: **Partitioning of Modular Equipment for Fault Isolation**

AUTHOR: **Sheskin, T.J.**

JOURNAL: Microelectronic Reliability - Vol 17, Pergamon Press Ltd. 1978

SCOPE: BIT diagnostic subsystem for military electronic equipment

PROBLEM DEFINITION: To investigate new approaches to the cost effective design of fault isolation procedures, with an objective to minimize the average costs associated with the repair.

CONSTRAINTS: Only primarv isolation to the module level is considered. Further isolation is by semiautomatic or manual methods.

APPROACH: The problem of partitioning the equipment into near optimum groups of modules such that average cost of isolating the faulty unit is minimum. Dynamic programming is used to derive weights for the groups of modules. This problem is formulated as a BINARY LINEAR PROGRAM. An outline procedure for assigning weights to groups is detailed. A sample calculation is enclosed.

The sample problem is partitioned into 3 groups by a binary program utilizing the group weights and is solved.

Solutions obtained by adding the group weights produced by dynamic programming for partitioning into 3 groups are compared with solutions for the minimum expected costs of testing these partitions. The details of the sample program and its calculations are tabularized.

COMPUTATIONAL EXPERIENCE: Solved example

CONCLUSIONS: The structure of a testing sequence formulated as a dynamic programming is shown.

The results also show that the sum of the group weights for a partition derived by dynamic programming provides a lower bound on the minimum expected cost of a testing sequence for that partition. This method emphasizes dynamic programming techniques to derive weights for the groups. Future research is recommended.

B-9

TITLE: Sequencing of Diagnostic Tests for Fault Isolation by Dynamic Programming

AUTHOR: Sheskin, Theodore J.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, No. 4, Dec. 1978.

SCOPE: BIT diagnostic subsystems for modular military electronic equipment

PROBLEM FORMULATION: BIT automatically executes a primary sequence of diagnostic tests to identify the groups of LRUs containing the faulty unit. Secondary isolation will be performed by semi-automatic or manual means through a suitable search procedure to minimize the expected cost. A sequence of tests is represented by a testing diagram and is optimized by probabilistic dynamic programming, in which the equipment states are treated as stages in a sequential decision process.

ASSUMPTIONS: Each LRU has a low probability of failure so that multiple failures are ignored.

COMPUTATIONAL EXPERIENCE: An equipment with 4 LRUs is considered and the minimum cost is worked out. The same example is extended to the use of dynamic programming, using recursive relationship.

CONCLUSIONS: The costs for running the BIT in deciding the faulty LRU and then that of identifying the faulty module are presented using dynamic programming. Though information gain and distinguishability criteria are good figures of merit, they fail to produce minimum cost sequences. A recursive procedure developed by Cohn and Ott and dynamic programming guarantee optimum testing sequence. These two procedures are proved to be equivalent. Examples are nicely formulated to illustrate this.

B-10

TITLE: Fault Isolation for Modular Electronic Equipment

AUTHOR: Sheskin, T.J.

JOURNAL: Proceedings of the 1979 Annual Reliability and Maintainability Symposium.

SCOPE: BIT diagnostic systems for military electronic equipment

PROBLEM DEFINITION: To minimize the average costs associated with the repair of electronic systems - to partition the equipment into mutually exclusive and exhaustive groups and to select a minimum cost set of BIT.

ASSUMPTIONS/CONSTRAINTS: A priori probability of failure of LRUs, given an equipment malfunction, is known.

SOLUTION APPROACH: BIT diagnostic identifies a failed LRU. A hybrid dynamic program is developed to solve both the problem of partitioning the equipment and selecting a minimum cost set of BIT. Secondary isolation is required for identifying the module. After application of a test, the state of the system is determined, from which a pass or fail decision is made.

COMPUTATIONAL EXPERIENCE: A sample problem is worked out in detail.

CONCLUSIONS: The computations of the hybrid dynamic programming are tabularized. Hybrid dynamic programming is an efficient procedure for determining both (1) the optimum partition of modular electronic equipment into mutually exclusive groups of LRUs and (2) the minimum cost set of BIT which produces this partition.

B-11

TITLE: A Method for Determining the Statistically Weighted Percent Fault Detection Coverage of a Self-Test Program

AUTHOR: Tasar, V. and Ohlef, H.L.

JOURNAL: Proceedings,1979 Annual Reliability and Maintainability Symposium

SCOPE: Structural fault detection coverage of self-test programs, designed to test digital circuits.

PROBLEM DEFINITION: Studying the effect of the probability of occurrence of faults on the percent fault detection coverage. A method used to find the percent structural fault detection coverage of a self-test program, and a method used to calculate the probability of occurrences of all faults are considered in the analysis.

ASSUMPTIONS:

1. A circuit node fails due to either a stuck at zero or a stuck at one fault.
2. Only one node can fail in the circuit at any given time.
3. The probability of failure of a node is equally distributed between the probability of occurrence of a stuck at zero and a stuck at one fault.

SOLUTION APPROACH: Mathematical analysis and probability distribution.

COMPUTATIONAL EXPERIENCE: The proposed method has been applied to a self-test program designed to test the CPU of the BDX-910 minicomputer,the results are presented and analyzed. The statistically weighted percent fault detection coverage is also calculated.

CONCLUSIONS:

1. A procedure is developed for combining the structural fault detection of a self-test program, designed to test a digital computer with the probability of occurrences of all the faults which have been analyzed to find the coverage.
2. A method is determined to calculate a statistically weighted percent fault detection coverage.

B-12

TITLE: Built-In-Test and External Tester Reliability Characteristics

AUTHOR: Tuttle, D.E., Loveless, R.

JOURNAL: RADC-TR-80-32, Final Technical Report, March 1980

SCOPE: Equipment with BIT/ETE. In particular aircraft electronic systems.

PROBLEM DEFINITION: To study the BIT/ETE reliability impact on prime equipment design and maintenance downtime.

SOLUTION APPROACH: Effectiveness of BIT is evaluated from field survey data by considering effectiveness measures. BIT is used for system monitoring, system checkout and for fault isolation to facilitate repair. Fault isolation gives the biggest recurns. A set of design trade-off equations produced using multiple regression techniques provide a high level of correlation for predicting actual test equipment failure. Since failure of ETE caused logic tie problems, the reliability attributes of external testers and BIT affect the systems reliability and life cycle cost.

Test equipment are classified as a) special purpose testers (for specific system, dedicated) b) general purpose testers.

40 LRU circuits are analysed to obtain design attributes for prime equipment of percent BIT and percent tested as related by failure rates. A technical discussion of BIT/ETE, reliability, effectiveness measures is presented along with a maintenance time distribution to indicate the alternate maintenance concepts employed.

CONCLUSIONS: Results of the use of field survey data to develop effectiveness measures are presented, along with applications. Addition of BIT to the LRU pays off as lower maintenance time/cost at a minimal decrease in equipment reliability. The range of BIT is a function of electronic circuitry. The study provides information on the basic relationship necessary for BIT/ETE evaluation. Design considerations that make BIT more effective are developed and enumerated. Further study is recommended in the field of software required to operate the system and to take advantage of the fact that the next generation of avionics employ microcircuitry.

B-13

TITLE: Optimal Allocation of Fault Detectors

AUTHOR: Takami, I. et al.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, no. 5, Dec., 1978.

SCOPE: Series systems with fault detectors to find component failures

PROBLEM DEFINITION: To minimize total cost of detectors and S-expected loss caused by system failure during T.

ASSUMPTIONS: Series system - Hence component failure implies system failure. Failure of components are S-independent. Fault detector is not perfect. Exponentially distributed component failure identification time. Constant failure rate (λ_i) and repair rate (μ_i).

SOLUTION APPROACH: A Markovian model and a case of a non-linear binary integer programming problem. An example is considered for series system. Generalization of the model is discussed.

COMPUTATIONAL EXPERIENCE: Integer programming iterations.

RESULTS AND CONCLUSIONS: Optimal allocation of fault detectors is determined.

B-14

TITLE: Diagnostic Development -- A New Prospective

AUTHOR: Linden, V.L.

JOURNAL: ATE Newsletter

SCOPE: Future weapon system

PROBLEM DEFINITION: To study the effectiveness of BIT/FIT and discuss approaches/trends towards highly automated diagnostics.

ASSUMPTIONS:

1. BIT eliminates need to teach system theory.
2. BIT reduces troubleshooting time.
3. BIT reduces support equipment requirements.

SUMMARY: Diagnostic specifications are to be written with a clear understanding of the methodology employed by the contractor in meeting them.

Occurrence of multiple faults, though rare, should not be ignored since deteriorated wiring (with age) can cause such problems and often leads to trouble. Cases of false alarms, could not duplicate (CND) and retest okay (RTOK) too are to be specified. These are to be kept to a minimum. False alarm, CND, RTOK are explained briefly.

Test results for E-3A, F-16 and EF-111A are included.

Diagnostic development should receive the same attention as development of equipment performance. Early involvement with the diagnostic system is suggested. Also, the diagnostic development should go hand in hand with the hardware design, in order to be more efficient.

The need for a 100% diagnostic capability is explained.

Finally, it is to be understood that the issue is diagnostic capability and not the degree of automation - of course a limit of the current technology.

RESULTS AND CONCLUSIONS: Highly trained personnel are not required to maintain a system capable of diagnosing itself. Hence the training imparted at the training center can be changed into a task-oriented one.

Recent evaluation of diagnostic systems confirm their below expected performance.

RESULTS AND CONCLUSIONS: (Continued)

It is highly recommended that specifications be performance oriented and not numerics.

A user should develop his requirements based on constraints and determine these operational and maintenance constraints. A 100% diagnostic capability (a mixture of automatic and manual) must be insisted on.

B-15

TITLE: Development of Built-In-Test Equipment for Tactical FM Radios

AUTHOR: W.W. Gaertner et al.

PREPARE FOR: Army Electronic Command AD: A005277

SCOPE: Design of BITE hardware for tactical FM Radios

SUMMARY: Goals to be met in the design included:

1. achievement of fault isolation to a replaceable module/ printed circuit card level.
2. minimization of BITE size, weight and power consumption
3. elimination of possible interaction with the radio set operation when the BITE unit is in operating, non-operating, or failure model.
4. continuous on-line monitor and press-to-test mode capabilities for fault detection.
5. acheivement of fault isolation through press-to-test mode.

The body of the paper describes the design of the BITE circuitry with photographs and schematics.

CONCLUSIONS:

1. Development specifications should clearly define the desired BITE characteristics.
2. There must be fully integrated design of both the operating circuitry and the BITE circuitry.
3. BITE circuitry should be replaced along with the operating circuitry in a given module.
4. Most test sequencing, evaluation and display circuitry can be implemented in CMOS technology.
5. BITE test sequencing, evaluation, and display circuitry should have a replaceable module by itself and should have self-test capability.
6. Production cost increase created by BITE inclusion can probably be kept under 10 percent.

B-16

TITLE: Automatic FD/FI Systems: Requirements and Testing

AUTHOR: Horkovich, James A.

JOURNAL: AFTEC Logistics Assessment Procedures Division, Kirtland AFB

SCOPE: Sophisticated aircraft weapon systems, with BIT/ATE.

PROBLEM DEFINITION: To relate test results to diagnostic system specifications and to discuss evaluation parameters to be utilized in specifying diagnostic requirements.

SUMMARY: FD/FI is employed to increase system availability and reduce manpower and training necessary for support. The limitations of FD/FI capabilities resulted in loss of confidence and great confusion. Future specifications should overcome these. Presently, each specification is interpreted in a number of ways, which increases confusion.

A thorough methodology required to evaluate FD/FI system should focus on
1. Single thread closed loop data system
2. MTTR tool
3. Relating numbers to meaningful criteria.
These three elements are briefly discussed.

MTTR can be split further as set up time, troubleshoot time, replace/repair time and checkout time. Only the second and fourth related to FD/FI capability. These analysis were conducted on aircraft systems.

For greater effectiveness, FD/FI systems are to be incorporated during the development and testing cycle and specification parameters should at least include:

*Percentage of addressable FD/FI
*Percentage of time correct FD/FI
*Overall, system (automatic mode) and system (manual) MTTR
*CND, RTOKs rate
*Percent of maintenance accomplished using manual and automatic modes
*System MTTR model
*Maintenance man-hours

RESULTS AND CONCLUSIONS: Diagnostic specifications are poorly written and grossly misunderstood. Major flaws are:
1. Poorly defined FD/FI percentage numbers.
2. No clear relationship between these numbers and the user's maintenance concept.

RESULTS AND CONCLUSIONS (Continued)

3. Non recognition of major failure modes by designers.

4. FD/FI requirements should henceforth be developed in an orderly, integrated fashion.

B-17

TITLE: JLC Panel on Automatic Testing - Subtask Descriptions

AUTHOR:

JOURNAL: March 1979

SCOPE: Automatic Testing Equipment

SUMMARY: Includes detailed subtask descriptions, categorized under

1) Management
2) Acquisition support
3) Testing Technology

The subtasks are described by their

Purpose - aim of the sub task
Approach - short term and long term, with phases
Milestones
Assignment - under DARCOM, NMC, AFLC or AFSC
Funding Requirements - for the various comand units
Service points of contract

B-18

TITLE: Study Plan for JLC Panel on Automatic Testing

AUTHOR:

JOURNAL: October 1978

SCOPE: Automatic testing equipment

SUMMARY: To define tasks that will consider all aspects of automatic testing (online, off line and weapon system testability), with efforts to generate policies and procedures applicable to DOD to optimize definitions, applications and support of automatic testing hardware and software in the system acquisition management process. To develop system engineering and logistic tools, techniques and guidelines to increase proper application of ATE in weapon systems.

SUMMARY OF TASKS: Divided into 3 categores

1. Management - To develop management policies, procedures, guidance and controls.
   a. Policy and procedure
   b. Documentation
   c. Career guidance
   d. Organizational structure
   e. Weapon System/AT/ADPE computer acquisition interfaces

2. Acquisition Support - To develop tools necessary to integrate AT elements into weapon systems
   a. Terminology and data exchange
   b. Testability guidelines
   c. Logistics
   d. Test programs sets
   e. Hardware interface
   f. Education and Training
   g. Testing Requirements
   h. AT acquisition

3. Testing Technology - To assist in Research and Development, test and evaluation programs to improve AT state-of-the-art.
   a. Software
   b. Automatic test generation
   c. Design for Testability
   d. Machinery testing
   e. New technology
   f. Education, training, and management aids
   g. Advanced ATE concepts

A detailed outline of each of these sub-tasks are included.

B-19

TITLE: Military Standards On-Aircraft, Fault Diagnosis, Sub-Systems, Analysis/Synthesis Of

AUTHOR: Department of Defense

JOURNAL: MIL-STD-1591, 3 January 1977

SCOPE: Built-in-Test

PROBLEM DEFINITION: Establishing a criteria for conducting trade studies to determine the optimal design for an on-aircraft fault diagnosis/ isolation system (at the flight line level of maintenance).

CONCLUSIONS: The contractor's studies shall include the following considerations:

a) Contract requirement
b) Failure modes and effects
c) Alternate system configurations
d) Alternate diagnosis/isolation method
e) Life cycle cost
f) Standardization of hardware and software

All analysis performed will be subjected to a sensitivity analysis to determine the effects of possible errors in the input data.

The contracts shall formulate conceptual options for the design of the OBBIT from the following inputs:

a) Contactual requirements
b) Primary system configuration
c) Primary system reliability data
d) Primary system FM & A

The most cost-effective option shall be selected. The most cost-effective option will be determined using a specified model which takes into account maintenance maintainability, reliability and cost characteristics.

Analysis shall be performed on the maintenance man-hours and the mean-time-to-repair requirements to determine:

1) The maximum permissible number of LRUs that may be isolated by a single set of diagnostics.
2) The average proportion of faults in each LRU or group of LRUs detectable by the diagnostics in question.
3) The reliability characteristics of each LRU.
4) Information such that the cost of each set of diagnostics can be calculated.

B-20

TITLE: Self-Diagnosing Design Techniques

AUTHOR: Heckelman, R.W., Knight, W.W., and Straub, W.W.

JOURNAL: Electronics Laboratory, General Electric, Publication Number AFAL-TR-78-183, Syracuse,N.Y., August 1981

SCOPE: Built in Tests

PROBLEM DEFINITION: The effects of architecture, functional partitioning, and module and component features on microprogrammable self-diagnosing capabilities of digital processors were investigated. These results were then used to create a set of design guidelines for designing self-diagnosing, fault-tolerant processors highly reliable microprocessors namely: monolithic and bit-slice processors using LSI devices. The microprocessor's execution speed, fault tolerance, and mission reliability were also studied.

COMPUTATIONAL EXPERIENCE: Two airborne applications were studied, they were; the fly-by-wire flight control processor and the synthetic operture group map function of an airborne multimode radar signal processor. Both applications were examined to determine the requirements, beginning with mission identification and functional analysis.

CONCLUSIONS: The study of the two applications led to the development of algorithm flow followed by performance analysis of representative tasks and resource sizing in terms of memory, processor speed and complexity as measured by the variety of operations and execution speed. These results are summarized in an Appendix.

The application of the guidelines strongly influences the design of the self-diagnosing fault tolerant processor (SDFTP). The architectural considerations are of primary importance in the design of a self-diagnosing processor particularly those making extensive use of large scale integrated circuits (LSI).

Utilization of redundancy for self diagnosis leads to an increase in the probability of failure and to the desirability of enhancing the reliability of the self-diagnosing processor design. Technological considerations dictate that redundancy be applied external to the device.

Partitioning of the processor designs should be based on hardware attributes, fault error models and type of diagnosis. Hardware attributes include partition function, structure regularity, size, speed and communication requirements.

CONCLUSIONS (Continued)

The guideline summary for a fault tolerant, self-diagnosing bit slice microprocessor is presented.

The SDFTP reliability is calculated to be four or five orders of magnitude better than the simplex processor for self-test coverage in the range of .9 to 1.0. Thus compared to the simplex processor design, the SDFTP is significantly superior for high fault-tolerant and high reliability applications with short mission time, such as the fly-by-wire electronic flight control processor. The SDFTP design can tolerate two faults and still provide undergraded operation, while the simplex process has no tolerance at all.

The advantages of a very reliable, fault tolerant, self-diagnosing LSI implemented design can be realized. Increasing the number of LSI devices and the degree of integration of the devices decreases the size, weight,and ultimately the cost. This approach enhances these advantages while accounting for the likelihood of LSI induced multiple-bit errors.

C - COMBINATIONAL CIRCUITS

C-1. Breuer, M.A. et al., "Identification of Multiple Stuck-Type Faults in Combinational Networks," IEEE Transactions on Computers, Vol. C-25 (1976).

C-2. Hayes, J.P., "Transaction Count Testing of Combinational Logic Circuits," IEEE Transactions on Computers, Vol. C-25 (1976).

C-3. Hornbuckle, G.D. and Spann, R.N., "Diagnosis of Single-Gate Failures in Combinational Circuits," IEEE Transactions on Computers, Vol. C-18 (1969).

C-4. Kamal, S., "An Approach to the Diagnosis of Intermittent Faults," IEEE Transactions on Computers, Vol. C-24 (1975).

C-5. Kautz, W.H., "Fault Testing and Diagnosis in Combinational Digital Circuits," IEEE Transactions on Computers, Vol. C-17 (1968).

C-6. Kohavi, Z. and Berger, I., "Fault Diagnosis in Combinational Tree Networks," IEEE Transactions on Computers, Vol. C-24 (1975).

C-7. Koren, I. and Kohavi, Z., "Sequential Fault Diagnosis in Combinational Networks," IEEE Transactions on Computers, Vol. C-26 (1977).

C-8. Preparata, F.P., "An Estimate of the Length of Diagnostics Tests," IEEE Transactions on Reliability, Vol. R-18 (1969).

C-9. Powell, T.J., "A Procedure for Selecting Diagnostic Tests," IEEE Transactions on Computers, Vol. C-18 (1969).

C-10. Weiss, C.D., "Bounds on the Length of Terminal Stuck-Fault Test," IEEE Transactions on Computers, Vol. C-21 (1972).

C-11 Goel, P., "An Implicit Enumeration Algorithm to Generate Tests for Combinational Logic Circuits," IEEE Transactions on Computers, Vol. C-30 (1981).

C-1

TITLE: Identification of Multiple Stuck-Type Faults in Combinational Networks

AUTHOR: Brewer, M.A., Chang, S.J., and Su, S.Y.H.

JOURNAL: IEEE Transactions on Computers, Vol. C-25, No. 1, Jan. 1976

SCOPE: Multiple stuck-type faults in combinational networks

PROBLEM DEFINITION: Identifying multiple stuck-type hardware failures in combinational switching networks, and introducing the concept of solving simultaneous equations over check point variables.

ASSUMPTIONS: Faults under consideration are only those defined at the check points.

SOLUTION APPROACH: Switching theory

COMPUTATIONAL EXPERIENCE: Solved example

CONCLUSIONS:

1. The check point solutions are studied in detail from which the function realized by a faulty circuit is calculated.
2. An on-line testing procedure is developed for constructing a test set for identifying a specific fault in a circuit to within an equivalence class.
3. It is also outlined how to apply these techniques to the following problems: a) identifying redundancy, b) determining the set of faults not detected by an arbitrary test set and, c) constructing a complete fault dictionary.

C-2

TITLE: Transition Count Testing of Combinational Logic Circuits

AUTHOR: Hayes, John P.

JOURNAL: IEEE Transactions on Computers, Vol. C-25, No. 6, June 1976.

SCOPE: Combinational circuits - Single and multiple stuck-at faults.

PROBLEM DEFINITION: To look into the feasibility of using transition count (TC) technique in fault detection.

CONSTRAINTS: Stuck-at faults only - not for intermittent faults.

APPROACH: Instead of recording the entire sequence R at a point P (as in conventional methods), C(R) is recorded in the number of times the signal at P changes value (from 1 to 0 or 0 to 1). This is compared to a predetermined C(Ro). If they differ, then it is interpreted suitability

$$C(R) = \sum_{i=1}^{m-1} (R_i + R_{i+1}) \text{ when } R = R_1, R_2, \ldots R_m$$

Advantage is that you need not record either the observed/ correct test response sequence R, hence basic test circuitry too is simplified.

Gray coded or pseudo random sequences are usually employed.

A formal analysis of TC testing is presented.

A heuristic rule for the design of TC tests - to maximize the fault coverage of a TC test(S), S should be constructed so that C(Ro) is either as large or as small as possible.

Necessary theorems and theory are developed on using the TC method in fault detection and isolation.

COMPUTATIONAL EXPERIENCE: A TC testing algorithm flow chart is given.

CONCLUSIONS: Generation of TC tests is basically a sequential process. Hence it is similar to conventional test generation for sequential circuits - ie. the order is important and certain test patterns may be repeated.

It needs more tests than conventional methods and detection is not guaranteed for all faults. An inefficient method, it doesn't detect all the tests conventional methods do. It needs slightly more tests than conventional methods. It doesn't provide complete fault detection in all cases.

The design of TC tests for sequential circuits appears to be quite difficult.

Other coding schemes, similar to this method have been suggested. The "run-count" is determined by finding the length of the longest sequence consisting of all ones or zeroes in a response sequence R. TC is also related to the concept of check sum - a widely used technique for detecting errors in data tables.

C-3

TITLE: Diagnosis of Single-Gate Failures in Combinational Circuits

AUTHOR: Hornbuckle, G.D., and Spann, R.N.

JOURNAL: IEEE Transactions on Computers, Vol. C-18, No. 3, March 1969

SCOPE: Single-gate failure in combinational circuits.

PROBLEM DEFINITION: Detecting and diagnosing arbitrary single-gate failures in combinational logic circuits.

ASSUMPTIONS: At most a single gate has failed.

SOLUTION APPROACH: Graph Theory

COMPUTATIONAL EXPERIENCE: Only one solved example is reported. However it is mentioned that a computer program is being written, and the computation time is also being investigated.

CONCLUSIONS:

1. Two procedures are presented for detecting and diagnosing arbitrary single-gate failure in combinational circuits. These procedures do not require the construction of a fault table and will locate, to within an equivalence class, the faulty gate and describe its failure.
2. The bounds derived for the size of the various test sets give an indication of the computation time and memory required for testing.

C-4

TITLE: An Approach to the Diagnosis of Intermittent Faults

AUTHOR: Kamal, S.

JOURNAL: IEEE Transactions on Computers, Vol. C-24, No. 5, May 1975.

SCOPE: Intermittent faults in combinational circuits.

PROBLEM DEFINITION: Developing a model for intermittent faults in combinational circuits as well as a detection procedure for the diagnosis of these faults.

ASSUMPTIONS:

1. The circuit is irredundant.
2. It is either fault free or it has only one of n possible intermittent faults.
3. A detection experiment has been run and proved that the circuit has an intermittent fault.

SOLUTION APPROACH: Probabilistic Model

COMPUTATIONAL EXPERIENCE: A flow chart for the suggested procedure and a solved example are presented.

CONCLUSIONS:

1. A procedure for the diagnosis of intermittent faults in combinational circuits is proposed. The procedure is based on the repeated application of tests that test for these faults had their effect been permanent.
2. The expected length of the diagnosis procedure is proved to be finite.
3. Necessary and sufficient conditions that the fault table must satisfy in order to obtain maximum diagnostic resolution are derived and compared with those needed in permanent fault case.

C-5

TITLE: Fault Testing and Diagnosis in Combinational Digital Circuits

AUTHOR: Kautz, W.H.

JOURNAL: 1st Annual IEEE Conference, IEEE No. 16C51, Sept. 1967 IEEE Transactions on Computers, Vol. C-17, No. 4, April, 1968.

SCOPE: Fault diagnosis in combinational digital circuits

PROBLEM DEFINITION: Devising economical test schedules for the testing and diagnosis of faults in combinational switching networks, including the following problems: 1) detection of whether any of a prescribed list of faults has occurred; 2) location of the particular fault; and 3) location of the fault within the limits of the module in which it has occurred.

ASSUMPTIONS: The fault condition to be detected or located is fixed (non-transient) in nature.

SOLUTION APPROACH: Mathematical analysis and matrices

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: Procedures are described for deriving minimal or near minimal test schedule for 1) the location of up to about 100 impossible faults 2) the detection of several hundred faults in any small to medium-sized combinational digital network.

C-6

TITLE: Fault Diagnosis in Combinational Tree Networks

AUTHOR: Kohavi, Zvi and Berger, Israel

JOURNAL: IEEE Transactions on Computers,Vol.C-24, No. 12, December 1975

SCOPE: Combination Tree Networks

PROBLEM DEFINITION: To generate minimal experiments to locate and diagnose faults in combinational tree networks - by adaptive and preset procedures.

CONSTRAINTS: Valid for tree network only, without using fault tables. Single, permanent, stuck-at-type faults only and irredundant fan-out free combinational networks, composed of basic gates (and, or, etc.). Equal probability of occurrence for all sets of equivalent faults is assumed.

SOLUTION APPROACH: Every fault-detection test defines a "failing" subtree which consists of the set of all the edges which were sensitized in the test. So that when the test fails, the fault is located within the failing subtree. These tests are so chosen to partition the failing subtree into subgraphs containing the sensitized and unsensitized edges. The intersection of all these subgraphs yields the location of the fault.

Procedure for adaptive experiments is given in detail followed by the preset experiments - these are longer than adaptive, but the advantage is that they are predefined.

An analogy between fault-location experiment and a binary code assigned to the set of distinguishable faults is shown. Hence, fault location is equivalent to constructing the required code.

CONCLUSIONS: The upper bound on the number of tests required to locate a fault within a graph is $N \leq \max (n_i | i = 1 . . . . k) + (\log_2(k+1))$

A procedure for determining such tests is presented. For the adaptive case, a complete binary diagnosing tree is always present.

C-7

TITLE: Sequential Fault Diagnosis in Combinational Networks

AUTHOR: Koren, I. and Kohavi,Z.

JOURNAL: IEEE Transactions on Computers, Vol. C-26, No. 4, April 1977.

SCOPE: Fault diagnosis in combinational networks

PROBLEM DEFINITION: Generating sequential decision trees (SDT's) for fault diagnosis in digital combinational networks. Mainly in decision trees containing minimal fault detection paths.

ASSUMPTIONS:

1. Faults under consideration are assumed to be:
   a) single b) permanent c) stuck at type fault.

SOLUTION APPROACH: Mathematical analysis

COMPUTATIONAL EXPERIENCE: Only solved examples

CONCLUSIONS:

1) A model is suggested in which different probabilities of occurrence can be assigned to the different faults.
2) In order to locate any fault, an SDT is generated directly from the structure of the network without using a fault table.
3) The structure of the network is presented in a simple tabular form called the gate table.
4) A lower bound for the cost function of the SDT is derived.
5) An explicit algorithm for generating an SDT is presented, this algorithm is restricted to fan-out-free networks.

C-8

TITLE: An Estimate of the Length of Diagnostic Tests

AUTHOR: Preparata, F.P.

JOURNAL: IEEE Transactions on Reliability, Vol. R-18, Aug. 1969

SCOPE: Test schedules in combinational networks

PROBLEM DEFINITION: Establishing bounds on the length of the shortest diagnostic schedule (a set of tests which allows fault identification) in a combinational network, which could be used as a guideline for the evaluation of heuristically or suboptimally computed test schedules.

ASSUMPTIONS:

1. A single output combinational network.
2. The generic test-fault matrix should be a random matrix.

SOLUTION APPROACH: Mathematical Analysis

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS:

1. Obtained is a lower bound on the distribution of the guaranteed test schedule length over the set of all the binary matrices which have distinct columns.
2. Obtained is an upper bound on the median of the test-schedule length.

C-9

TITLE: A Procedure for Selecting Diagnostic Tests

AUTHOR: Powell, T.J.

JOURNAL: IEEE Transactions on Computers, Vol.C-18, No. 2, February 1969.

SCOPE: Combinational Circuits

PROBLEM DEFINITION: To select from a given set of near optimal group of tests for diagnosis to the package level, avoiding exhaustive trials of large numbers of test combinations.

ASSUMPTION: At any given time, no more than one fault is present and it is fixed (well defined), not intermittent. A priori probabilistic weight of each test is given initially for the circuit.

APPROACH: Each test is given a weight - based on a priori probability and ability to partition the network that is yet to be partitioned. A fault table is constructed. Probabilistic weights are listed. The test which has the highest probalistic weight is applied first and so on. An iterative formula is mentioned for this.

CONCLUSIONS: A programmable procedure for finding a good set of tests that will diagnose a given combinational circuit has been presented. Since the procedure is based on probabilistic weights, a near-optimal set of tests is selected.

C.10

TITLE: Bounds on the length of Terminal Stuck-Fault Tests

AUTHOR: Weiss, C.D.

JOURNAL: IEEE Transactions on Computers, Vol. C-21, No. 3, March 1972

SCOPE: Terminal Stuck-Fault Tests

PROBLEM DEFINITION: Determining whether the externally available terminals of a network or circuit realizing an n-place switching function are logically stuck-at-1 or stuck-at-0, that is, whether the network is functioning as if one or more input terminals or the output terminals is always fixed at a logical 1 or logical 0 independent of the actual input combination applied. Also finding bounds on the size of the optimal test as a function of the number of input terminals is discussed.

SOLUTION APPROACH: Switching Functions

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS:

1. An efficient algorithm for finding minimum length terminal stuck-fault test is developed.
2. It is proved that for $n \leq 5$ a least upper bound on the test length is $n + 1$, and for $n > 5$ an upper bound is $2n-4$.
3. A greatest lower bound is 3, for all $n > 1$.

C-11

TITLE: An Implicit Enumeration Algorithm to Generate Tests for Combinational Logic Circuits

AUTHOR: Goel, P.

JOURNAL: IEEE Transactions on Computers, Vol. C-30, No. 3, March 81

SCOPE: Combinational Circuits

PROBLEM DEFINITION: Developing a new algorithm PODEM (path-oriented decision making) to generate tests for combinational circuits using an implicit enumeration approach analogous to that used for solving 0-1 integer programming problems. The problem is formulated as the search of an n-dimensional 0-1 state space constraint using a set of Boolean constraints.

SOLUTION APPROACH: Branch and Bound Algorithm

COMPUTATIONAL EXPERIENCE: 15 different cases were used to compare the performance of both PODEM and the D-algorithm (DALG)

CONCLUSIONS:

1. PODEM is very efficient for the class of combinational logic circuits that is used to implement error correction and translation (ECAT) functions, and is significantly more efficient than DALG over the spectrum of combinational logic circuits.
2. PODEM is a simple and complete algorithm that will generate a test if any exist.

D - REDUCTION TECHNIQUES AND COVERING PROBLEMS

D-1. Du, M.W., "A Way to Find a Lower Bound for the Minimal Solution of the Covering Problem," IEEE Transactions on Computers, Vol. C-21 (1972).

D-2. Friedman, A.D., "Comment on 'A Method for the Selection of Prime Implicants,'" IEEE Transactions on Electronic Computers, Vol. EC-16 (1967).

D-3. Gimpel, J.F., "A Reduction Technique for Prime Implicants Tables," IEEE Transactions on Electronic Computers, Vol. EC-14 (1965).

D-4. Hadlock, F., "On Finding a Minimal Set of Diagnostic Tests," IEEE Transactions on Electronic Computers, Vol. EC-16 (1967).

D-5. Hayes, J.P., "On Realizations of Boolean Functions Requiring a Minimal or Near Minimal Number of Tests," IEEE Transactions on Computers, Vol. C-20 (1971).

D-6. Rao, C.V.S. and Biswas, N.N., "Minimization of Incompletely Specified Sequential Machines," IEEE Transactions on Computers, Vol. C-24 (1975).

D-7. Robinson, S.U. III and House, R.W. "Gimpel's Reduction Technique Extended to the Covering Problem With Costs," IEEE Transactions on Electronic Computers, Vol. EC-16 (1967).

D-8. Slagle, J.R. et al., "A New Algorithm for Generating Prime Implicants," IEEE Transactions on Computers, Vol. C-19 (1970).

D-9. Vink, B. et al., "Reduction of CC-Tables Using Multiple Implication," IEEE Transactions on Computers, Vol. C-27 (1978).

D-10. Agarwal, V.K. and Masson, G.M., "A Functional Form Approach to Test Set Coverage in Tree Networks," IEEE Transactions on Computers, Vol. C-27 (1979).

D-11 Phillips, M.J., "K-out-of-n: G Systems are Preferable," IEEE Transactions of Reliability, Vol. R-29 (1980).

D-1

TITLE: A Way to Find a Lower Bound for the Minimal Solution of the Covering Problem

AUTHOR: Du, Min-Wen

JOURNAL: IEEE Transactions on Computers, Vol. C-21, No. 3, March 1972

SCOPE: Covering Problem

PROBLEM DEFINITION: Deriving a lower bound for the size of a minimal solution of a 0-1 covering problem. Given a 0-1 matrix C = (C_{ij}) called a covering matrix, we say that row i covers column j if C_{ij} = 1. The covering problem is to find a minimal number of rows so that all columns can be covered.

SOLUTION APPROACH: Mathematical Programming

COMPUTATIONAL EXPERIENCE: Solved example

CONCLUSIONS: A lower bound for the minimal solution of the covering problem is derived.

D-2

TITLE: Comment on "A Method for the Selection of Prime Implicants"

AUTHOR: Friedman, A.D.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-16, No. 2, April 1967.

SCOPE: Prime Implicants

SUMMARY: Luccio's procedure to simplify the prime implicant table covering problem is discussed. Though it can be formulated as a linear integer programming problem, it is not advised since it doesn't completely solve the problem but merely simplifies the integer linear programming problem.

Luccio's procedure is used to determine the minimal cover for the original prime implicant table. Then, the remaining problem is to be solved by the 3 classical reduction procedures (row and column dominance and row essentiality without recourse to linear integer programming).

Luccio's example is considered and the method explained.

A heuristic for handling the cyclic prime implicant table is then presented.

Since cyclic prime implicant tables very often collapse if a few rows can be selected, it is suggested to use the above procedure, which frequently leads to a complete solution without branching or integer programming.

D-3

TITLE: A Reduction Technique for Prime Implicants Tables

AUTHOR: Gimpel, J.F.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-14, No. 4, Aug 1965.

SCOPE: Boolean functions (sum of product expressions)

PROBLEM DEFINITION: To select a subset of prime implicants which includes the fundamental minterm.

APPROACH: The covering problem is defined. The covering problem is represented algebraically instead of in prime implicant table form. Various terminologies associated with column reduction are defined (weight of a column, plural covering problems, reducing column of the first kind, etc.)

If a covering problem is not plural, then it is regarded as not having any reduced columns.

A method for reduction of columns of the first kind is illustrated as an algorithm. A detailed example is considered.

A technique for reduction of columns of the second kind is presented also.

COMPUTATIONAL EXPERIENCE: Algorithmic, hence can be written as a program.

CONCLUSIONS: A reduction step about a reducing column of the second kind produces a new table having one row less than the original table and one row less in a minimal cover. Hence a reduction is obtained. Previous reduction techniques had failed miserably when dynamic/integer linear programming was used for 9 or more variables, suggesting the need for a new reduction technique. Possibly, this method could be of use in such situations.

D-4

TITLE: On Finding a Minimal Set of Diagnostic Tests

AUTHOR: Hadlock, Frank

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-16, No. 5, Oct. 1967.

PROBLEM: To formulate the problem of minimizing the set of diagnostic tests as a prime implicant problem.

CONSTRAINTS: A data matrix is constructed. It is a matrix of rows (faults) and columns (tests). A test t_i distinguishes between two faults if the two rows are different. A set distinguishes such faults if there is any test in the set which can detect the fault.

The role of prime implicants is played by the diagnostic tests. The role of minterms of the Boolean function by pairs of faults associated with components from different packages and which are distinguished from one another by the parent set.

A prime implicant table is constructed and the minimal test covering of the fault pair is to be determined by one of the many methods available.

Examples are presented to illustrate this fact.

COMPUTATIONAL EXPERIENCE: None

CONCLUSION: This is a less formidable method than constructing all possible test diagrams at the same time yielding a minimal test set.

D-5

TITLE: On Realizations of Boolean Functions Requiring a Minimal or Near-Minimal Number of Tests

AUTHOR: Hayes, John P.

JOURNAL: IEEE Transactions on Computers, Vol. C-20, No. 12, December, 1971

SCOPE: Combinational logic circuits

PROBLEM DEFINITION: To design combinational logic circuits such that they require a minimal or near minimal number of tests.

CONSTRAINTS/ASSUMPTIONS: Stuck at faults are assumed.

APPROACH: The bounds on the number of tests required by various network structures are considered. The distribution of the number of fault detection tests required by 2-level realizations are examined - for most functions of n variables, 2n-1 tests are required. Four measures of diagnosability are used. Bounds on the minimum number of tests required, a function of the number of inputs to the largest fanout-free subnetwork is considered. Necessary theorems are developed for this.

An example of a 23 input circuit is considered and the bounds discussed and a procedure for determining the minimum number of tests for numerous cases/examples are considered. Multi-level realizations are included.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: For an input fanout-free network, the number of single and multiple fault detection tests is between $2\sqrt{n}$ and n + 1, while for fault location, it is between $2\sqrt{n}$ and 2 n. Any linear function can be realized by a cascade circuit, which not only requires few tests, but is such that a complete set of detection tests can be generated recursively, without detailed analysis of the circuit.

If a function possesses some structure such as linearity or functional separability there exist multilevel realizations requiring very few tests. For any linear function, there exists a dignosable multilevel realization. The trade off is with large numbers of logic levels.

D-6

TITLE: Minimization of Incompletely Specified Sequential Machines

AUTHOR: Rao, C.V.S. and Biswas, N.N.

JOURNAL: IEEE Transactions on Computers, Vol. C-24, No. 11, November, 1975

SCOPE: Sequential machine like computers, digital communication systems and control systems.

PROBLEM: To develop an efficient algorithm for minimizing ISSM, which is also a simple and a programmable one.

ASSUMPTION/CONSTRAINT: Maximal compatibles are assumed available.

SOLUTION APPROACH: Compatibles that do not belong to any minimal solution are identified and then deleted. Such deletion theorems and generation of symbolic compatibles are explained. A set of "primary compatibles" is made first. Compatibles are detected if 1) they are unimplied compatibles, 2) the closure class set of elements of compatibles cover at least one state which belongs to that compatible. 3) If $(I_i U N_i) \subset C_i$ then C_i is deleted.

I_i = Implied part of a compatible C_i

N_i = Uncovered part of a compatible C_i

Those compatibles that cannot be deleted are called "Basic Compatibles". An example to generate basic compatibles is considered. A method to delete the compatibles recursively is explained. A procedure for generation of symbolic compatibles is given in detail. Initialization of the cardinality of a nominal closed cover is discussed, based on finding a minimal closed cover containing only maximal compatibles. Additional techniques, based on the rank of compatibles, to reduce computational work are discussed.

COMPUTATIONAL EXPERIENCE: The algorithm is recursive so that it can be computerized.

CONCLUSION: The theorem proves that there exists a minimal closed cover which is a collection of symbolic compatibles only. Those compatibles which cannot be members of any mimimal closed cover are deleted. Since this is done as part of the first stage in the process of minimizing an ISSM, we will be left with a relatively small set of compatibles only.

CONCLUSION (Continued)

A simple, efficient and systematic method for small/medium sized machines, it can be used for hand computation.

Converges faster to the final solution than other methods involving generation of prime closed sets.

D-7

TITLE: Gimpel's Reduction Technique Extended to the Covering Problem With Costs.

AUTHOR: Robinson, S.U. III, and House, R.W.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-16,No. 4, Aug. 1967.

SCOPE: Covering Problem

PROBLEM DEFINITION: Given A, an array of 0's and 1's, and C, a vector of positive numbers, it is required to find a least cost covering for A. The problem is solved by first solving a derived problem (A_1, C_1) and then adding a row index to this solution using a derived rule. The technique was conceived by Gimpel for the covering problem with all costs equal 1. But it is solved here for the general case.

ASSUMPTION: The problem has a reducing column; a column in the array A which 1) has precisely two 1's in two rows of equal cost, and 2) dominates no other columns in A.

SOLUTION APPROACH: Boolean algebra

COMPUTATIONAL EXPERIENCE: Four solved examples

CONCLUSIONS: A new reduction technique conceived by Gimpel is shown to solve any covering problem with costs that has a column with exactly two 1's, in rows of equal cost.

D-8

TITLE: A New Algorithm for Generating Prime Implicants

AUTHOR: Slagle, J.R. et al.

JOURNAL: IEEE Transactions on Computers, Vol. C-19, No. 4, April, 1970

SCOPE: Combinational circuits

PROBLEM DEFINITION: To describe an algorithm which generates all the prime implicants of a Boolean function.

SOLUTION APPROACH: The algorithm is based on frequency ordering on literals. The truth table is converted to obtain a conjunctive normal form. The algorithm is explained by considering an example.
The flow chart of the algorithm is given. Additional examples are solved to illustrate the method. After obtaining the prime implicants, the same algorithm is used to minimize the Boolean function. The detailed procedure and the results as applied to the original problem are presented.
The algorithm doesn't generate repeated clauses, thus saving computer time.

COMPUTATIONAL EXPERIENCE: The algorithm is implemented by a computer program in the LISP language.

CONCLUSIONS: The algorithm may also generate some non-prime implicants. The algorithm may be used to find the minimal sums of a Boolean function. It doesn't generate the same prime implicant more than once.
The algorithm is different from those previously given, and in many cases more efficient.
The Boolean function need not be presented in canonical form.

D-9

TITLE: Reduction of CC-Tables Using Multiple Implication

AUTHOR: Vink, B. et al.

JOURNAL: IEEE Transactions on Computers, Vol. C-27, No. 10, October, 1978

SCOPE: Boolean functions

PROBLEM: To reduce the covering closure tables using multiple implications

SOLUTION APPROACH: The CC table is an extension of the prime implicant of Quine-McCluskey's and can handle certain forms of covering problems having a non-additive cost function. A solution to a CC-table is a closed cover of minimum cost. The reduction of CC-table using multiple implication is presented. The prime permissible implicants (PPI) are generated, the content of the CC-table is determined and the dominated tail rows are removed to obtain the reduced CC-tables. Closure column reduction is applied to columns which are covered by the same tail rows. Essential tail rows are defined. Definitions of the cover column implication, ex-closure column implication, PPI row dominance, essential PPI rows are given.

COMPUTATIONAL EXPERIENCE: A computer program for the minimization of TANT networks was written for IBM 36/50 in APL.

CONCLUSIONS: The program accepts a specification of a function and calculates the result with the algorithm of our choice. Various proofs of the theorems used in reduction techniques are given as an appendix. The introduction of multiple implication causes the number of closure columns to be strongly reduced. Moreover, some closure columns change into an ex-closure column, reducing the CC-table further.

D-10

TITLE: A Functional Form Approach to Test Set Coverage in Tree Networks

AUTHOR: Agarwal, V.K. and Masson, G.M.

JOURNAL: IEEE Transactions on Computers, Vol. C-27, No. 1, January 79

SCOPE: Set Coverage

PROBLEM DEFINITION: Developing an approach to establishing the existence of a certain fault interrelationship relative to test set coverage in tree networks which is based only on the form of the output function.

ASSUMPTIONS: Only primary input fanout can exist.

SOLUTION APPROACH: Boolean Algebra

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: A procedure is given to describe the form of a boolean function generically by means of L-expressions. Certain types of L-expressions on a given set of lines in the network are related to the complete coverage of all multiple faults on those lines by test sets explicitly designed to cover only single faults on those lines.

D-11

TITLE: K-out-of-n: G Systems are Preferable

AUTHOR: Phillips, M.J.

JOURNAL: IEEE Transactions of Reliability, Vol. R-29, No. 2, June 80

SCOPE: Partitioning Problem

PROBLEM DEFINITION: Proving the validity of the K-out-of-n: G systems compared to parallel series networks with the same number of components for all values of n

ASSUMPTIONS:

1. The system consists of n i.i.d. components
2. A component is either operating or idle.
3. The components are subject to two mutually exclusive failure modes (stuck-at idle, and stuck-at operate)
4. The components are neither totally reliable nor unreliable.

SOLUTION APPROACH: Probabilistic Approach

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The k-out-of-n: G systems are shown to be preferable to any other coherent systems when: a) the i.i.d. components have two failure modes and b) the criterion used for deciding preference is a linear function of the probability of the system failing to idle.

M - MULTIPLE FAULTS

M-1. Allan, F.J. et al., "An Approach to the Diagnosability Analysis of a System," IEEE Transactions on Computers, Vol. C-24 (1975).

M-2. Fujiwara, H. and Kinoshita, K., "Connection Assignment for Probabilistically Diagnosable Systems," IEEE Transactions on Computers, Vol. C-27 (1978).

M-3. Hakimi, S.L. and Amin, A.T., "Characterization of Connection Assignment of Diagnosable Systems," IEEE Transactions on Computers, Vol. C-23 (1974).

M-4. Happ, W.W. and Sarkisian, E., "Combination Techniques for Fault Identification in Multiterminal Networks," 1968 Annual Symposium on Reliability.

M-5. Karunanithi, S. and Friedman, A., "Analysis of Digital Systems Using a New Measure of System Diagnosis," IEEE Transactions on Computers, Vol. C-28 (1979).

M-6. Kime, C.R., "An Analysis Model for Digital System Diagnosis," IEEE Transactions on Computers, Vol. C-19 (1970).

M-7. Luccio, F., "Reduction of the Number of Columns in Flow Table Minimization," IEEE Transactions on Electronic Computers, Vol. EC-15 (1966).

M-8. Maheshwari, S.N. and Hakimi, S.L., "On Models for Diagnosable Systems and Probabilistic Fault Diagnosis," IEEE Tranctions on Computers, Vol. C-25 (1976).

M-9. Mandelbaum, D., "A Measure of Efficiency of Diagnostic Tests Upon Sequential Logic," IEEE Transactions on Electronic Computers, Vol. EC-13 (1974).

M-10. Meyer and Masson, "An Efficient Fault Diagnosis Algorithm for Symmetric Multiple Processor Architectures," IEEE Transactions on Computers, Vol. C-27 (1978).

M-11. Nakano, H. and Nakanishi, Y., "Graph Representation and Diagnosis for Multiunit Faults," IEEE Transactions on Reliability, Vol. R-23 (1974).

M-12. Preparata, F.B. et al., "On the Connection Assignment Problem of Diagnosable Systems," IEEE Transactions on Electronic Computers, Vol. EC-16 (1967).

M-13. Russell, J.D. and Kime, C.R., "System Fault Diagnosis: Masking, Exposure, and Diagnosability Without Repair," IEEE Transactions on Computers, Vol. C-24 (1975).

M-14. Deo, N., "Self Diagnosability of a Computer," IEEE Transactions on Electronic Computers, Vol. EC-15 (1966).

M-15. Toida, S., "System Diagnosis and Redundant Tests," IEEE Transactions on Computers, Vol. C-25 (1976).

M-16. McPherson, J.A. and Kime, C.R., "A Two-Level Diagnostic Model for Digital Systems," IEEE Transactions on Computers, Vol. C-27 (1979).

M-17. Fujiwara, H. and Kinoshita, K., "On the Computational Complexity of System Diagnosis," IEEE Transactions on Computers, Vol. C-27 (1978).

M-18. Risse, T., "On the Structure of Self-Diagnosing Systems," Methods of Operations Research, Vol. 43.

M-1

TITLE: AN APPROACH TO THE DIAGNOSABILITY ANALYSIS OF A SYSTEM

AUTHOR: Allan, F.J. et al.

JOURNAL: IEEE Transactions on Computers, Vol. C-24, No. 10, October 1975.

SCOPE: t-diagnosable systems. Systems represented as a digraph.

PROBLEM DEFINITION: To present a theorem which covers all the aspects of system diagnosis.

CONSTRAINTS:

1. The condition of the system does not change during the tests.
2. Each unit is either faulty or not faulty.
3. No units test themselves.
4. The most likely event is that the minimum number of units are faulty.

SOLUTION APPROACH: The testing arrangements of a system are formulated as a digraph G(v,e); v is a set of nodes representing units and e is a set of edges representing test connections.

The conditions to be satisfied by the diagnosis are mentioned. A necessary and sufficient condition for a system to be t-diagnosable is formulated as a theorem. Using this theorem, previous results are derived in a unified way.

$\tau(G)$, the diagnosability number is defined as a function of the partitions of the node set.

Then a system is t-diagnosable iff $t \geq \tau(G)$ (number of faulty units). Theorems are derived to specify the limits of $\tau(G)$.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The system represented by a digraph. G(v,e) is t-diagnosable iff $t \leq \tau(G)$.

Upper and lower limits of $\tau(G)$ are proved.

A simple characterization of t-diagnosable systems is obtained. An advantage of this method is that it yields results obtained previously in the literature.

M-2

TITLE: CONNECTION ASSIGNMENTS FOR PROBABILISTICALLY DIAGNOSABLE SYSTEMS

AUTHOR: Fujiwara, H. and Kinoshita, K.

JOURNAL: IEEE Transaction on Computers, Vol. C-27, No. 3, March 1978.

SCOPE: Automatic fault diagnosis for digital systems with multiple faults.

PROBLEM DEFINITION: Finding the necessary and sufficient conditions for a system to be diagnosable with at most t faults. The system is made up of a number of units. Each unit is assumed to be tested by some other unit.

ASSUMPTIONS: All components are not equiprobable which requires taking into consideration the probabilistic nature of the occurrence of faults.

SOLUTION APPROACH: Graph-theoretic model

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS:

1. Developing necessary and sufficient conditions for the existence of a connection to form probabilistically t-diagnosable systems with and without repair.

2. Presenting two nonoptimal designs for probabilistically t-diagnosable systems with and without repair.

M-3

TITLE: CHARACTERIZATION OF CONNECTION ASSIGNMENT OF DIAGNOSABLE SYSTEMS

AUTHOR: Hakimi, S.L., and Amin, A.T.

JOURNAL: IEEE Transactions on Computers, Vol. C-23, No. 1, January 1974.

SCOPE: t-diagnosable and multiple faults.

PROBLEM DEFINITION: A system S capable of automatic fault diagnosis consists of n units and a prescribed connection assignment that assigns each unit to test a subset of other units. Given the set of test outcomes, the problem is to identify all faulty units in S.

SOLUTION APPROACH: Graph Theoretic

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The necessary and sufficient conditions for a system S to be t-diagnosable are presented and proved in a series of theorems and lemmas.

Finding an efficient algorithm for identifying faulty units in S remains an open problem.

The test outcome which equals I is redundant for a t-diagnosable system.

M-4

TITLE: COMBINATORIAL TECHNIOUES FOR FAULT IDENTIFICATION IN MULTI-TERMINAL NETWORKS

AUTHOR: Happ, W.W. and Sarkisian, E.

JOURNAL: 1968 Annual Symposium on Reliability.

SCOPE: Multi-terminal devices - semiautomatic and automatic fault identification techniques.

PROBLEM DEFINITION: To provide

1) Systematic approach to the derivation and clarification of the formulae and theorems used.

2) Algorithms for computer oriented calculations for the identifications of unique circuit functions.

3) Utilization of unique circuit functions for the diagnosis of faults of internal components from an optimum set of external measurements.

ASSUMPTIONS: Nonredundant circuits.

SOLUTION APPROACH: Uses combinatorials. All the terms used in the paper are listed and explained. Recursion formulae are mentioned to calculate the number of configurations obtainable from external terminals and connected graphs. Properties of a few of the parameters are given (of the number of distinct s-separated post configurations). An illustrative example is listed.

The sequence of calculations of the combinational network is given in the form of a flow chart.

COMPUTATIONAL EXPERIENCE: Computer programming of the various recursive formulae has been suggested.

CONCLUSIONS: A flow chart of operations suitable for computer programming is given. A good number of illustrative examples are attached. Results are formulated to yield algorithms for computer oriented procedures to identify the complete set of non-redundant configurations of a multi-term network. Future investigations and present developments are mentioned. Project FIST pinpoints the defective element and allow its replacement in contrast to semi-automatic techniques which only say "good" or "bad" about a module.

M-5

TITLE: ANALYSIS OF DIGITAL SYSTEMS USING A NEW MEASURE OF DIAGNOSIS

AUTHOR: Karunanithi, S. and Friedman, Arthur D.

JOURNAL: IEEE Transactions o Computer, Vol. C-28, No. 2, February 1979.

SCOPE: Digital Systems; Sequential circuits.

PROBLEM DEFINITION: To study the diagnosability of digital systems using t/s diagnosability.

CONSTRAINTS: Probability of 'i' faulty units is > probability of (i+1) faulty units. Deterministic faults and faults are stable during applications of the test.

SOLUTION APPROACH: One step t/s diagnosability and sequential t/s diagnosability are investigated.

K-step diagnosability is defined. Definitions as to when the system is diagnosable and optimal are included.

Theorems to characterize single loop systems are mentioned, with proof. One step and sequential diagnosabilities of single loop systems and $D_{\delta a}$ systems are explained. $D_{\delta a}$ - A system in which there exists a test link from unit u_i to u_j iff $(j-i) \bmod n = \delta \cdot m \bmod n$; $\delta < n$. Various strategies for the above two systems are mentioned, for optimal system design.

All the repair strategies are compared and the tradeoffs between the number of units replaced and the number of tests iterations performed are discussed. Suitable examples are worked out.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: Two canonical classes of systems - single loop systems and
$D_{\delta a}$ systems are examined based on the above 2 categories of diagnosability. Single loop system design, using minimum number of test links possible, appear to have more desirable attributes than others.

This method incorporates the concept of possible replacement of fault-free units in systems repair.

M-6

TITLE: AN ANALYSIS MODEL FOR DIGITAL SYSTEM DIAGNOSIS

AUTHOR: Kime, Charles R.

JOURNAL: IEEE Transactions on Computers, Vol. C-19, No. 11, Novermber 1970.

SCOPE: LSI systems with multiple deterministic faults.
(more suited for design states)

PROBLEM DEFINITION: To present models for the diagnostic test-fault relationships and to transform one form to another. Also, to assess the diagnostic capability of the test set.

CONSTRAINTS/ASSUMPTIONS: A set of n possible faults can occur. Faults are deterministic and solid during the application of the set of tests. Multiple faults are allowed.

SOLUTION PROCEDURES: Previous models proposed for relating faults to diagnostic tests are discussed briefly. Tests are differentiated as complete and incomplete. The evaluation of the capability of the test set τ in diagnosing the fault set F under the conditions given by F & G is expressed as resolutions. Certain definitions in this regard have been included. Procedures for determining resolutions are given - both for the 1st order and 2nd order resolutions. Theorems on resolvability and conditions of irresolvability have been added.

The 2nd order resolution itself includes in it the 1st order resolutions. The procedure for determining the 2nd order resolution is mentioned in the form of an algorithm. Diagnosability - a closely related concept of resolution is explained. An example is considered and the conditions and parameter values resulting are tabulated.

This fault q-cube concept is then extended to higher systems with more than just 0,1, and don't care states.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: There is a inherent trade off between complexity of representation and analysis and diagnostic information-because of the nature of the model and the fact that it can be used to represent complex system faults in a simple fashion. Thus diagnostic information loss is computed. A helpful model in the design stages more than in an actual on-line diagnosis situations.

M-7

TITLE: REDUCTION OF THE NUMBER OF COLUMNS IN FLOW TABLE MINIMIZATION

AUTHOR: Luccio, F.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-15, No. 5, Oct. 1966.

SCOPE: Sequential Networks.

PROBLEM DEFINITION: To show that even column reductions can be considered to advantage in minimizing an incompletely specified machine and present the basic concepts of reduction technique.

APPROACH: Two columns are replaced by a third one if for every input sequence n_k, the input sequence n^1_k resulting from n_k by replacing the two columns by a new column, yield an output sequence identical to the one obtained by applying n_k. By considering maximal compatibles, it is shown that column reductions may not always be possible. Hence, by choosing compatibles suitably, a form is obtained in which a column can be eliminated. This is shown by considering two examples.

"Compatibility class of columns" is defined in the same way as that of rows.

A generalized cover (g-cover) τ,4 = a set 'τ' compatible rows and a set '4' of compatible columns

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: A low cost sequential network is obtained by considering non-trivial column reductions too. This is true if the number of inputs is not assigned in the problems.

By column reductions, not only is the already 'reduced number of states' taken to advantage, but also the number of inputs driving the system is reduced to obtain the same output sequence hence minimizing costs.

M-8

TITLE: ON MODELS FOR DIAGNOSABLE SYSTEMS AND PROBABILISTIC FAULT DIAGNOSIS

AUTHOR: Maheshwari, S.N. and Hakimi, S.L.

JOURNAL: IEEE Transactions on Computers, Vol. C-25, No. 3, March 1976.

SCOPE: Automatic fault diagnosis for digital systems with multiple faults.

PROBLEM DEFINITION: Finding the necessary and sufficient conditions for a system to be diagnosable with at most T faults. The system is made up of a number of units. Each unit is assumed to be tested by some other units.

ASSUMPTIONS: All components are not equiprobable which required taking into consideration the probablistic nature of the occurrence of faults.

SOLUTION APPROACH: 0-1 integer programming formulation, duality theory of linear programming, and graph-theoretic model.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS:

1. Introducing a diagnosability measure t based on the probability of occurrence of faults.

2. Developing necessary and sufficient conditions to diagnose any fault set whose probability of occurrence is greater than t (without repair).

M-9

TITLE: A MEASURE OF EFFICIENCY OF DIAGNOSTIC TESTS UPON SEQUENTIAL LOGIC

AUTHOR: Mandelbaum, David

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-13, No. 5, Oct. 1964.

SCOPE: Sequential Machines.

PROBLEM DEFINITION: To define a function J which measures the efficiency of a given configuration of output sensors as compared with another configuration on the otherwise identical machine M.

ASSUMPTIONS: All components have equal probability of failures. Every faulty machine can be reset to a known initial state-a reset condition.

SOLUTION APPROACH: The requirements of 'J' are mentioned and it is shown that they are satisfied by the entropy function of communication theory.

$$J \equiv -\sum_{i}^{k} \frac{di}{N} \log_2 \frac{di}{N} = -\sum_{i}^{k} n_i \log_2 n_i \ .$$

Where the machine M is composed of N components, d_i is the number of faulty machines in a set of faulty machines S_i, and $\frac{di}{N} = n_i$

Properties of J are listed

An example showing that J is better than another measure is given.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The entropy function of communication theory is a more desirable measure of efficiency of a diagnostic test.

M-10

TITLE: AN EFFICIENT FAULT DIAGNOSIS ALGORITHM FOR SYMMETRIC MULTIPLE PROCESSOR ARCHITECTURES

AUTHOR: Meyer and Masson

JOURNAL: IEEE Transactions on Computers, Vol. C-27, No. 11, Nov. 1978.

PROBLEM DEFINITION: To develop an algorithm for determining the existing fault situation in a symmetric multiple processor architecture, given its testing results.

ASSUMPTIONS: n-processors are present, each of which is tested by at least t others and at most t others are faulty. The interconnection design is the so called $D_{1,t}$ design (where a testing inter-connection from u_i to u_j (modules) occur if and only if j-i=m, m=1,...t. If a module is fault free, then the corresponding table it generates is correct.

SOLUTION APPROACH: A test B_i has components B_{ij} when B_{ij} represents the conclusions of module u_i regarding the state of module u_j to be fault free, then $B_{ij} = 0$, else = 1.

Then, an efficient table B_o, B_1,...B_{n-1} is attempted to be constructed such that table B_i reflects accurately the fault situations of the multiprocessor architecture. A detailed algorithm is presented with a flow chart to interpret when a module u_i is not faulty. Conversely, it is also shown that if module u_i is fault free, then the table B_i reflects the actual fault situations.

An accelerated algorithm is explained which is suited for parallel implementations on a network of N microprocessors. An example is considered with n=9 modules and t=3.

COMPUTATIONAL EXPERIENCE: The algorithm can be implemented as a program in a microprocessor based system.

CONCLUSIONS: The second algorithm is suitable for implementation even in a microprocessor like Intel 8085 - for n=8, t=2, it needs 176 bytes. The table B_i are constructed independently of the others. Hence computations are increased. Any scheme to decrease computations will increase the complexity of the coding.

Ideally suited for a fault diagnostic of $D_{1,t}$ network.

M-11

TITLE: GRAPH REPRESENTATION AND DIAGNOSIS FOR MULTIUNIT FAULTS

AUTHOR: Nakano, H. and Nakanishi, Y.

JOURNAL: IEEE Transactions on Reliability, Vol. R-23, No. 5, December 1974.

SCOPE: Diagnosis of Multiple Faults.

PROBLEM DEFINITION: Detecting and locating a multiunit fault in a system consisting of a number of functionally connected units.

SOLUTION APPROACH: Graph theory. A rectangular diagnostic matrix is derived from a graph representation of a system. An algorithm is developed for constructing a square reachability matrix from the diagnosis matrix. A graph derived from the reachability matrix permits diagnosis of multiunit faults.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: A graphical method has been developed for the diagnosis of system faults which can include multiunit faults. Two patterns could be used, either 1-step diagnosis or sequential diagnosis. A sequential diagnosis permits the isolation of any combination of multiunit faults.

M-12

TITLE. ON THE CONNECTION ASSIGNMENT PROBLEM OF DIAGNOSABLE SYSTEMS

AUTHOR: Preparata, F.P., Metze, G., and Chien, R.T.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-16, No. 6, Dec. 1967.

SCOPE: Automatic fault diagnosis for systems with multiple faults.

PROBLEM DEFINITION: The problem is automatic fault diagnosis for systems with multiple faults. The system is decomposed into different units. By means of a given arrangement of testing links (connection assignment) each unit of the system tests a subset of units and a proper diagnosis can be arrived at for any diagnosable fault pattern. Both sequential and instantaneous (one-step) diagnosis procedures have been treated in detail.

SOLUTION APPROACH: A graph-theoretical models

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS:

1. Necessary and sufficient conditions are obtained for any procedure to be multiple-fault diagnosing.
2. A variety of methods are derived for the optimal assignment of testing links.

M-13

TITLE: SYSTEM FAULT DIAGNOSIS: MASKING, EXPOSURE, AND DIAGNOSABILITY WITHOUT REPAIR

AUTHOR: Russell, J.D. and Kime, C.R.

JOURNAL: IEEE Transactions on Computers, Vol. C-24, No. 12, December 1975.

SCOPE: Diagram of multiple faults without repair.

PROBLEM DEFINITION: Considering the diagnosability without fault repair of a digital system containing at most t-faults. Two parameters are defined, the masking and exposure indices. Conjoined with the previously defined closure index, the parameters fundamentally characterize the capability for executing valid tests in a multiple fault environment. The necessary and sufficient conditions for a system to be t-fault diagnosable without repair are to be derived.

SOLUTION APPROACH: Mathematical models.

COMPUTATIONAL RESULTS: Two solved examples.

CONCLUSIONS:

1. By employing a model previously proposed, parameters called the masking index and exposure indices are defined which along with the closure index characterize, in a fundamental manner, the capability for executing valid tests in the presence of faults.

2. General results are given which permit determination of the diagnosability without repair of a system containing at most t faults on the basis of the defined parameters.

3. The levels of diagnosability particularly beyond 1-fault diagnosability are not generally obtained without a substantial amount of redundancy in the hardware.

M-14

TITLE: THE SELF DIAGNOSABILITY OF A COMPUTER

AUTHOR: Deo, Narsingh

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-15, No. 5, October 1966.

PROBLEM DEFINITION: To define a figure of merit to measure the self-diagnosability of a system.

CONSTRAINTS: A priori probability of failures is known. If not available, equiprobable failure is assumed.

SOLUTION APPROACH: Besides a main processor, the system has a small/mini machine capable of (programatically) detecting and locating a fault in the processor. A list of all tests set $T = \{T_1, T_2, \ldots T_n\}$ such that every failure in the system makes one or more of these tests fail is chosen. The set of failures is $F = \{F_1, F_2, ..F_m\}$. By taking the intersections of the sets of suspects for the failing test case $T_{i1}, T_{i2}, ..T_{ir}$, the fault F_j is pinpointed. Resolution of the systems is defined in terms of the number of suspected modules to be replaced. Resolution R is maximum when every failure can be traced down exactly to one module and minimum when the routine only detects but does not locate the fault.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: A look up table approach. Points to a set of modules to be replaced rather than the faulty one.

Resolution $$R = \sum_{i=1}^{m} k_i \Big/ \sum_{i=1}^{m} k_i^2$$

Where k_i = the number of suspected modules under F_i

Also $R_{min} = \frac{1}{n}$ and $R_{max} = 1$

A totally dedicated microcomputer/microprocessor is needed to run the fault routines.

M-15

TITLE: SYSTEM DIAGNOSIS AND REDUNDANT TESTS

AUTHOR: Toida, S.

JOURNAL: IEEE Transactions on Computers, Vol. C-25, No. 11, November 1976.

SCOPE: Diagnosis of multiple faults.

PROBLEM DEFINITION: Introducing the concept of redundant tests in relation to the diagnosability of a system to see its effect on previous algorithms to determine the diagnosability.

SOLUTION APPROACH: Graph-theoretic

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS:

1. The study reveals that there is a chance of improving the efficiency of the previous algorithms to determine the diagnosability.
2. The study also suggests a way to improve the diagnosability of a system by adding an extra test.

M-16

TITLE: A TWO-LEVEL DIAGNOSTIC MODEL FOR DIGITAL SYSTEMS

AUTHOR: McPherson, J.A. and Kime, C.R.

JOURNAL: IEEE Transactions on Computers, Vol. C-27, No. 1, January 1979.

SCOPE: t-part diagnosability and t-part detectability.

PROBLEM DEFINITION: Detecting and locating faulty parts in digital systems including defining parameters which are to be used in models to determine conditions for detectability, t-part diagnosability with and without repair.

ASSUMPTIONS: The maximum number of simultaneously occurring faults within a given faulty part can be less than the total number of functional units contained in the part.

SOLUTION APPROACH: Graph theoretic approach.

COMPUTATIONAL EXPERIENCE: Solved examples

CONCLUSIONS: A two-level diagnostic model has been defined. The part level at which detectability and diagnosability are defined and the fault level at which testing is performed and at which functional units or portions thereof are defined. This model allows diagnosis at the level of replacement in digital systems. Part closure, part masking, and occupancy degree are defined and used in defining conditions for t-part detectability, t-part diagnosability with and without repair.

M-17

TITLE: ON THE COMPUTATIONAL COMPLEXITY OF SYSTEM DIAGNOSIS

AUTHOR: Fujiwara, H. and Kinoshita, K.

JOURNAL: IEEE Transactions on Computers, Vol. C-27, No. 10, October 1978.

SCOPE: Multiple Faults.

PROBLEM DEFINITION: Analyzing the computational complexity of system diagnosis for both cases of sequential fault diagnosis and single loop systems.

SOLUTION APPROACH: Graph theoretic

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The computational complexity of fault diagnosis in self diagnosable systems is discussed. Several problems for instantaneous and sequential fault diagnosis of systems are polynomially complete and for single-loop systems these problems are solvable in polynomial time.

M-18

TITLE: ON THE STRUCTURE OF SELF-DIAGNOSING SYSTEMS

AUTHOR: Thomas Risse

JOURNAL: Methods of Operations Research, Vol. 43.

SCOPE: t-diagnosability for various models of fault-tolerant self-diagnosing computer systems.

ASSUMPTIONS:

(1) the system is partitioned into n autonomous units

(2) each unit may only be distinguished as totally fault free or not.

(3) the state of the system is described by a binary vector of length n.

(4) the units of the system are capable of testing each other.

SOLUTION APPROACH: A test graph with units as nodes and test connections as arcs describes the testing relationships. Based on the interpretation of the tests and whether the graph is directed or undirected, three models are given. For each a characterization theorem of t-diagnosability is given.

One of the models is then generalized to consider a test structure in which a set of units can commonly evaluate the state of the system. A characterization theorem of t-diagnosability is proved for this.

EXAMPLES:

(1) PLURIBUS system (Katsuki et al.) three processors each with a bus to each of the two main memories.

(2) A duplex computer system (McPherson, Kime).

R - SYSTEM RELIABILITY

R-1. Ben-dov, Y., "Optimal Testing Procedures for Coherent Systems," AD-A057952 (1977).

R-2. Biegel, J.E. and Bulcha, B., "Multilevel Modularization of Systems to Minimize Life Cycle Cost," RADC-TR-78-207, Final Report (1978).

R-3. Chang, H.Y., "Figures of Merit for the Diagnostics of a Digital System," IEEE Transactions on Reliability, Vol. R-17 (1968).

R-4. Conley, G.A., "Digital System Diagnostics - Design/Evaluations," 1980 Proceedings of the Annual Reliability and Maintanability Symposium.

R-5. Consolla, W.M. and Danner, F.G., "An Objective Printed Circuit Board Testability Design Guide and Rating System," RADC-TR-79-327, Final Report (1980).

R-6. Cook, T.N., "Analysis of Fault Isolation Criteria/Techniques," 1980 Proceedings of the Annual Reliability and Maintainability Symposium.

R-7. DeCorlieu, J., "Maintainability Diagnosis Techniques," 1966 Annual Symposium on Reliability.

R-8. Eble, F.A., "Maintenance Strategies for Ambiguous Faults," Index Serial Number 1072.

R-9. Johnson, R.A. and Brulê , J.D., "Diagnosis of Equipment Failures," RADC-TR-60-67A, Final Report Part I/II (1960).

R-10. Kuo, W. et al., "A Note on Heuristic Methods in Optimal System Reliability," IEEE Transactions on Reliability, Vol. R-27 (1978).

R-11. Nakagawa, Y. et al., "Optimal Reliability Allocation by Branch and Bound Technique," IEEE Transactions on Reliability, Vol. R-27 (1978).

R-12. Pau, L.F., "Specification of an Automatic Test System vs an Optimum Maintenance Policy and Equipment Reliability," IEEE Annual Reliability and Maintainability Symposium (1979).

R-13. Rose, J., "Fault Tolerant System Optimization," 1980 Proceedings of the Annual Reliability and Maintainability Symposium.

R-14. Tillman, F.A. et al., "Determining Component Reliability and Redundancy for Optimum System Reliability," IEEE Transactions on Reliability, Vol. R-26 (1977).

R-15. Tillman, F.A. et al., "Optimization Techniques for System Reliability with Redundancy - A Review," IEEE Transactions on Reliability, Vol. R-26 (1977).

R-16. Weisberg, S.A. and Schmidt, J.H., "Computer Technique for Estimating System Reliability," 1966 Annual Symposium on Reliability.

R-17. Williams, J.W. and Angell, J.B., "Enhancing Testability of Large-Scale Integrated Circuits Via Test Points and Additional Logic," IEEE Transactions on Computers, Vol. C-22 (1973).

R-18. Hecht, H., "Fault Tolerant Software," IEEE Transactions on Reliability, Vol. R-28 (1979).

R-19. Cox, G.W. and Carroll, B.D., "Reliability Modeling and Analysis of Fault-Tolerant Memories," IEEE Transactions on Reliability, Vol. R-27 (1978).

R-20. Coppola, A., "Taming the All-Equipment Reliability Test," IEEE Transactions on Reliability, Vol. R-27 (1970).

R-21. Willoughby, W., $\overline{R}$, Quality.

R-22. Wright, D.K. et al., "F-16 Follow-on Operational Suitability Test and Evaluation", Air Force Test and Evaluation Center, Kirkland AFB, New Mexico, 87117.

R-23. Controller General - GAO, "Effectiveness of U.S. Force can be Increased Through Improved Weapon System Design - A Report to the Congress, PSAD 81-17.

R-24. Pau, L.F., "Application of Pattern Recognition To Failure Analysis and Diagnosis," Human Detection and Diagnosis of System Failures (1980), Ruskilde, Denmark.

R-25. McCluskey, E.J., "Testing and Diagnosis of Logic", EURO IFIP (1979).

R-1

TITLE: OPTIMAL TESTING PROCEDURES FOR COHERENT SYSTEMS

AUTHOR: Ben-dov, Yosi

JOURNAL: Sept. 1977, AD-A 057952

SCOPE: Coherent Systems

PROBLEM DEFINITION: To minimize the expected cost of testing a coherent system. The concept of importance of components is used to develop branch and bound algorithms which determine the optimal testing policy for any coherent system.

ASSUMPTIONS:

1) Each component functions or fails independently of any other
2) Cost for testing and a priori probability that a component is failed are given.

APPROACH: Reliability importance of components is mentioned and the reasoning behind the algorithms is explained. He defines the 'unimportance' of a component. The branch and bound algorithm is explained in detail. The process is flow charted. An example is considered in which the step by step details of the algorithm are given. The rationale of the algorithm is explained.

Reliability functions for three systems are discussed. They are

1. Series system
2. Parallel systems
3. 2 out of 3 systems - (A special case of k out of n systems is calculated)

An optimal tree is developed to point to the component to be tested first. Based on the results of this test, it branches to the next twig. Subtrees are developed such that at each iteration, the subtree on hand has the lowest bound for the expected cost. The algorithm flow chart is presented.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The concept of importance of components and their cost of testing is well presented.

R-2

TITLE: MULTILEVEL MODULARIZATION OF SYSTEMS TO MINIMIZE LIFE CYLCE COST

AUTHOR: Biegel, J.E. and Bulcha, B.

JOURNAL: RADC-TR-78-207, Final Technical Report, September 1978.

SCOPE: Electronic equipment with modularizations.

PROBLEM DEFINITION: To develop a new procedure on the modularization or partitioning of electronic equipment such that the life cycle cost is minimum.

ASSUMPTIONS/CONSTRAINTS: Failures among modules, sub-assemblies and assemblies are independent of one another.

APPROACH: The system is decomposed into functional elements, then reconstructed into modules - to form a sub-assembly and higher level sub-assembly, etc. To do this, the graph of the network is used to generate proper cuts. An example problem is included. The network to be analyzed is represented as a sparse matrix.

A cost model for higher level design involving sub-assemblies and assemblies is developed. The acquisition cost of a multilevel design is split up into the cost of its modules, sub-assemblies and assemblies. A suitable spares allocation policy is chosen. Finally, using the cost models, spares allocation policy and inventory costs, an expression for the life cycle cost for a single equipment is developed.

COMPUTATIONAL EXPERIENCE: A computer program to modularize large networks is included. A description of the main program, subroutines for sorting, MTTR, LCC, spares allocations, maximizing availability/cost ratio, etc. are included. Also included is a subroutine to form the n x n interconnections matrix from the network data. A detailed program listing is in the appendix.

CONCLUSIONS: A method for modularizing large networks subject to physical, MTTR and availability contraints is developed, with a suitable spares allocations procedure.

A solutions methodology for higher level assemblies is obtained by repeated use of the procedure for lower level designs with appropriate modifications.

R-3

TITLE: FIGURES OF MERIT FOR THE DIAGNOSTICS OF A DIGITAL SYSTEM

AUTHOR: Chang, H.Y.

JOURNAL: IEEE Transactions on Reliability, Vol. R-17, No. 3, September 1968.

SCOPE: Any large system. The Bell Telephone System's No. 1 Electronic Switching System has been chosen as an example.

PROBLEM STATEMENT: To discuss accuracy and resolution of a diagnostic procedure and to see how their figures can be improved.

SOLUTION APPROACH: A dictionary of diagnostic test results of known faults is used in a "look up table."

1. A logic description of a machine is simulated and compiled into a computer program. A fault can then be suitably introduced by simply changing the program description.
2. Instead, physical simulations are done on the machine and the diagnostic tests are run and the result recorded.

Accuracy and resolvability - these two figures of merit are explained in detail. The bulkiness of the system, the type of message to be printed out and possible trade offs are discussed.

COMPUTATIONAL EXPERIENCE: A program of the logic simulations of the system is needed. An IBM 7094 program is used.

CONCLUSIONS: Accuracy (indicator of the fault detectability of a system's diagnostic procedure) can be improved by reducing the number of faults in the inconsistent category. An accuracy vs resolvability diagram is shown, (if the design objective is to isolate the fault to six or fewer circuit-packages, the central pulse distributor and the call store units of No. 1 ESS system performed better - from the example considered). Two figures of merits are discussed, accuracy and resolution. One can be improved at other's expense, unless some sacrifice is done in the diagnostic program itself. The author suggests two levels of dictionaries for this, each one having one of these two figures of merits, but not the other.

R-4

TITLE: DIGITAL SYSTEM DIAGNOSTICS - DESIGN/EVALUATIONS

AUTHOR: Conley, G.A.

JOURNAL: 1980 Proceedings Annual Reliability and Maintainability Symposium

SCOPE: For a complex digital data systems, using diagnostics.

PROBLEM DEFINITION: Specifications: 98% of failures detected.

90% of them isolated to one pluggable assembly.

Describe the 'failure modes and effect analyses' (FMEA) on a data system.

APPROACH: Makes a preliminary diagnostic prediction (PDP) based on estimates of the effectiveness of hardware/software diagnostic techniques. Explains the steps in FMEA, its detail-partitions, modes, affects, fault detection/isolation, posting, assessment, probability determination, severity, compensating provisions and finally diagnostic prediction of failures. After FMEA, the fault insertion is done physically to simulate faults (hundreds of them) the diagnostic tools are tested. Based on this performance, additional test points may have to be included.

COMPUTATIONAL EXPERIENCE: None

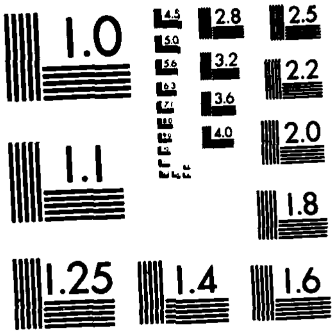
CONCLUSIONS: The end results of the integrated FMEA, diagnostics-design/ evaluation are a more useful FMEA, an improved diagnostic design and a maintainability demonstration test portraying the future maintenance characteristics of the systems.

Performance of 98.1% detection, 95.4% of isolation has been achieved by this method - using hardware/software and manual techniques.

The FMEA process block diagram is interesting. Sometimes, manual/human observations and procedures are very effective in minimizing wasteful or unnecessary BIT.

AD-A126 167 ANALYTICAL PROCEDURES FOR TESTABILITY(U) OKLAHOMA UNIV 3/4
NORMAN SCHOOL OF INDUSTRIAL ENGINEERING A A ALY ET AL.
JAN 83 RADC-TR-83-4 F30602-81-C-0012

UNCLASSIFIED F/G 14/2 NL


1.0
4.5
5.0
5.6
6.3
7.1
8.0
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

P-5

TITLE: AN OBJECTIVE PRINTED CIRCUIT BOARD TESTABILITY DESIGN GUIDE AND RATING SYSTEMS

AUTHOR: Consolla, W.M. and Danner, F.G.

JOURNAL: RADC-TR-79-327, Final Report, January 1980.

SCOPE: Digital Printed Circuit Boards (PCB) - sequential synchronous/ asynchronous.

PROBLEM DEFINITION: To develop a testability design guide showing how to correct PCB testability problems, resulting in cost effective design and lower test programming.

SOLUTION APPROACH: A PCB from the B-1 aircraft program is considered as an example. Testability factors to be considered are listed. A revised evaluation system is proposed with classification into 1) basic factors, 2) positive factors 3) negative test factors. Parameters under these factors are listed.

Flip flop circuits are redesigned to give good testability. Importance is given to their controllability and observability. Minute sequential logic and bottle neck designs are modified to improve testability. Good documentation is stressed. A rating system is developed and used for each factor to evaluate the PCB testability. Cost effectiveness is considered.

A PCB circuit is chosen for demonstration and its testability analyzed. Next the PCB is modified as suggested earlier and the vast improvement in testability is shown.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The guide provides maximum advance testability information about a circuit, with the constraint that the testability evaluation and correction process is not to exceed 8-10 man hours. The initial high cost helps in reduced production test costs and reduced subsequent field maintenance.

It is emphasized what is to be done at the PCB circuit level to correct a design and make it testable.

R-4

TITLE: DIGITAL SYSTEM DIAGNOSTICS - DESIGN/EVALUATIONS

AUTHOR: Conley, G.A.

JOURNAL: 1980 Proceedings Annual Reliability and Maintainability Symposium

SCOPE: For a complex digital data systems, using diagnostics.

PROBLEM DEFINITION: Specifications: 98% of failures detected.

90% of them isolated to one pluggable assembly.

Describe the 'failure modes and effect analyses' (FMEA) on a data system.

APPROACH: Makes a preliminary diagnostic prediction (PDP) based on estimates of the effectiveness of hardware/software diagnostic techniques. Explains the steps in FMEA, its detail-partitions, modes, affects, fault detection/isolation, posting, assessment, probability determination, severity, compensating provisions and finally diagnostic prediction of failures. After FMEA, the fault insertion is done physically to simulate faults (hundreds of them) the diagnostic tools are tested. Based on this performance, additional test points may have to be included.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The end results of the integrated FMEA, diagnostics-design/ evaluation are a more useful FMEA, an improved diagnostic design and a maintainability demonstration test portraying the future maintenance characteristics of the systems.

Performance of 98.1% detection, 95.4% of isolation has been achieved by this method - using hardware/software and manual techniques.

The FMEA process block diagram is interesting. Sometimes, manual/human observations and procedures are very effective in minimizing wasteful or unnecessary BIT.

R-6

TITLE: ANALYSIS OF FAULT ISOLATION CRITERIA/TECHNIQUES

AUTHOR: Cook, T.N.

JOURNAL: 1980 Proceedings: Annual Reliability & Maintenance Symposium.

SCOPE: All systems of Aircraft except AVIONICS and ARMAMENTS.

PROBLEM DEFINITION: To develop an improved approach to the Fault Isolation Maintenance Data for complex non-avionics.

SOLUTION APPROACH: Failures and failure symptoms are defined. CH-54 helicopter is chosen as a model and its maintenance data analyzed in detail. A Fault Isolations and Analysis Technique (FIAT) is developed and is explained in detail with task flows, consisting of

a. Functional analysis
b. Failure mode analysis
c. Description of fault isolation task candidates
d. Review and consolidation and editing.

Each part is explained in detail.

COMPUTATIONAL EXPERIENCE: FIAT consists of two PL/1 programs and a number of utility sort routines.

CONCLUSIONS: Results of the survey are described. One-third of the symptoms are common for all aircrafts. One-half of these are observed via instruments.

1. FIAT data processing flow is tested.
2. A sample set of data is attached.
3. Future efforts are explained.

Fault isolation is a significant factor in cost of operating. Single most important cause is the poor quality of trouble shooting data in technical manuals. FIAT is an improvement for this. The task flow can be applied to other systems too.

R-7

TITLE: MAINTAINABILITY DIAGNOSIS TECHNIQUES

AUTHOR: De Corlieu, J.

JOURNAL: 1966 Annual Symposium on Reliability.

SCOPE: For any instrument, for proper maintenance, a good diagnosis is needed. Several diagnostic techniques are discussed. Incorporated monitoring instruments are favored rather than test consoles alone.

PROBLEM DEFINITION: Define customers' requirements in terms of availability and MTBF. Defines the qualities of a diagnosis and when it is needed.

APPROACH: Several techniques are described - four diagnosis techniques.

1. Entropic method. Something like a successive approximation method in D/A converters.
2. Decreasing probability method - Here pairwise non interfering tests can be done simultaneously to save time.
3. Linear Analysis technique.
4. Theory of sets and diagnosis techniques - defines errors from faults. Solves two examples - (a) for an extractor associated with long range radar (b) digital computers. A test program is run. Every deviation from a known result is interpreted - (say the test is all zeros or all ones loaded to register) then run a specialized program to single out the suspected assembly. On the other hand, if the failure results in the computer being non operable, then this gets classified under entropic method. A three stage amplified example is illustrated.

During the design stage, importance should be given to future diagnosis. Easy access should be a criterion for electrical measurements/tests.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: What about Marginal Checking Methods? The appendix shows how a minor change at the design stage can increase equipment maintenance by allowing the use of a simple diagnosis technique. It is emphasized to forsee diagnosis methods at the design stage itself.

R-8

TITLE: MAINTENANCE STRATEGIES FOR AMBIGUOUS FAULTS

AUTHOR: Eble, F.A

JOURNAL: Index Serial, No. 1072

SCOPE: Application of FARO < Fault Ambiguity Repair Optimization > computer program to group replacement strategy, to reduce the impact of fault ambiguity on availability.

PROBLEM DEFINITION: Describe FARO and show how to use it effectively for a large process. Say a computer with thousands of replaceable units.

ASSUMPTIONS:

1. Probabilistic failure rate of each card is known. This only speeds up the process.
2. The optimization function F (Q,T) is determined beforehand.

APPROACH: Suppose there are 1000 cards. Instead of testing each one for failure, group them in terms of units of 100 cards and find the culprit unit. Do the same for one unit. Say 10 separate sub units, and then finally locate the faulty card. A very fast method, i.e., each strategy subdivides the group into a "replacement set" configuration. For practical purposes 'N' is chosen as 15, i.e., 15 main groups. FARO evaluates all possible replacement set configurations for the specified card removal sequence, and calculates the expected values of Q = average number of cards removed per failure, T = average card interchange time + system checkout time.

FARO needs fault group size, replacement sequence, card failure ratio, interchange time, checkout time as input data. Multiple card units dramatically reduce program running time. The 'S' different strategies are chosen based on the proximity of card locations within the sets, standardization of card types within sets and uniformity of set size.

From sample FARO print out,

1. Low Q strategy more replacement sets than low T strategy.
2. The lower the system checkout time, the more compatible Q and T are.
3. Multicard units yield excellent savings in computer time with a very small loss of optimization.

APPROACH (Continued)

The article also speaks about Q-T problem, and results of a 10 years OARS simulation is attached. A calculation for availability is mentioned. Also, the quality effects of spares are discussed.

COMPUTATIONAL EXPERIENCE: FARO is discussed. Its sample print out is attached. OARS is mentioned. It is a Monte Carlo computer program. FARO is written in Fortran IV.

CONCLUSIONS: FARO offers a worthwhile payoff thorugh optimized replacement strategy. A good discussion of importance of Q and T and the trade off is made. Hence they are minimized in various ways - O, T, AT, QT^2, etc., depending on the installation needs.

R-9

TITLE: DIAGNOSIS OF EQUIPMENT FAILURES

AUTHOR: Johnson, R.A. and Brulè, J.D.

JOURNAL: RADC-TR-60-67A, Final Report, Part I of II, April 1960.

SCOPE: General, any system.

PROBLEM DEFINITION: To study the effect of various maintenance procedures on the overall reliability of an equipment.

SOLUTION APPROACH: The measures of performance - reliability, continuance, mean time to first failure, mean time to failure, availability are defined and described. failures are classified as: (a) Random failures, (b) Catastrophic Failure, (c) Random Temporary Failure. Specific mathematical models for these failure modes are postulated, and each model is explained in detail.

It is shown that based on life tests of a large number of elements, the life curve of most of these elements is exponential. The measures of performance are calculated by straightforward applications of probability theory.

Maintenance procedures depend on the method of diagnosis employed. Maintenance procedures considered are of the

1) Failure indicator type.
2) Periodic replacement of all elements.
3) Periodic replacement of elements in turns.

Analysis is performed for each of the 3 modes above with an aim at calculating the reliability measures. The results are plotted on graphs in the appendix: (reliability, availability and improvements). Relationship between mean time to failure and reliability function is derived.

Improvement of an order of magnitude is possible with sufficient maintenance. Each maintenance model differs considerably in its effect on the various measures of system performance.

CONCLUSIONS: Introduction of redundancy doesn't result in a significant increase in system mean life. Increasing the maintenance is a better solution than introducing a high degree of redundancy. Halving the maintenance period gives greater improvement than doubling the redundancy. For significant improvement in system performance, it is necessary to replace/repair each element in a time, short compared with the mean of the elements.

R-10

TITLE: A NOTE ON HEURISTIC METHODS IN OPTIMAL SYSTEM RELIABILITY

AUTHOR: Kuo, W. et al.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, No. 5, December 1978.

PROBLEM DEFINITION:

1. To critically review heuristic methods for solving optimum system reliability problems.
2. To extend one of them for solving non series-parallel systems reliability problems.

PROCEDURE: The problem to be solved is stated in each heuristic method discussed (6 of them). Sharm & Venkateswaran approach, Misra's approach, Aggarwal's approach, Nakagawa-Nakashima's approach, Tillman et al.'s approach, extended Nakagawa-Nakashima's approach (which the author adopts) and Uskhakov's approach are dealt with. Each one is later compared with the other one. Though heuristic approaches do not guarantee a global optimal solution, they are quite efficient compared to integer programming or dynamic programming approaches for complex systems optimization.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: The extended Nakagawa and Nakashima approach is quite efficient and general. This approach incorporates some of the previous ideas and solves general non-series-parallel systems.

The simplicity and efficiency of this approach is an asset in solving large practical problems.

R-11

TITLE: OPTIMAL RELIABILITY ALLOCATION BY BRANCH-AND-BOUND TECHNIQUE

AUTHOR: Nakagawa, Y., Nakashima, K. and Hattori, Y.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, No. 1, April 1978.

SCOPE: System Reliability.

PROBLEM DEFINITION: Finding the optimal solution of reliability allocation problems having multiple nonlinear constraints regardless of separability.

SOLUTION APPROACH: The problem is formulated as an integer nonlinear programming problem and the solution is based on branch and bound technique and developed by considering separation and relaxation techniques.

COMPUTATIONAL EXPERIENCE: Three examples were solved. All of which have been solved by another method in previous articles. The procedure was coded and run on FACOM 230/75 digital computer. It is proved that the proposed procedure is more efficient than other methods (execution time is less than other methods).

CONCLUSIONS: An efficient algorithm for finding the optimal solution of reliability allocation problem is presented and its efficiency is proved.

R-12

TITLE: SPECIFICATION OF AN AUTOMATIC TEST SYSTEM VS AN OPTIMUM MAINTENANCE POLICY AND EQUIPMENT RELIABILITY

AUTHOR: Pau, L.F.

JOURNAL: IEEE Annual Reliability and Maintainability Symposium, 1979.

SCOPE: Equipment Reliability and Maintenance.

PROBLEM DEFINITION: Studying the effect of the ATS performances on a decision rule among the alternatives repair and overhaul in the case of a catastrophic failure detected by an automatic test system so as to minimize the expected maintenance costs per unit of operational availability.

ASSUMPTIONS: The system is assumed to operate continuously until either it undergoes a check-out without removal or it is improperly pulled down for accessability considerations to other equipments.

SOLUTION APPROACH: Markov Model

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: A maintenance strategy is proposed. It minimizes the mean maintenance costs per unit time of operational life between unscheduled maintenance.

R-13

TITLE: FAULT TOLERANT SYSTEM OPTIMIZATION

AUTHOR: Rose, J.

JOURNAL: Proceedings, 1980 Annual Reliability an' Maintainability Symposium.

SCOPE: Design decisions of fault tolerant system h as aircraft, which can be applied to any large sy ns.

PROBLEM DEFINITION: To develop a cost optimum comprehensive of digital systems. To find MTTR.

CONSTRAINTS: A priori knowledge of certain statistics of the components is required.

APPROACH: The cost benefit design optimization model (CBDOM) for fault tolerant flight control systems is explained. A block diagram of the closed loop cost benefit optimization is included - uses certain statistically generated data for man hours, delay hours, quality of spaces, fuel saved, etc.

Next the fault tolerant system economics are discussed.

COMPUTATIONAL EXPERIENCE: Monte-Carlo simulation is mentioned as an effective method for analysis of reliability. SIMSCRIPT model of the system was found to match excellently.

CONCLUSIONS: Whether or not an aircraft after a certain number of flight hours can be dispatched without repair to certain components is well analyzed. Higher levels of redundancies and replication for system reliability is advocated (due to the advent of LSI).

R-14

TITLE: DETERMINING COMPONENT RELIABILITY AND REDUNDANCY FOR OPTIMUM SYSTEM RELIABILITY

AUTHOR: Tillman, F.A., Hwang, C.L. and Kuo, W.

JOURNAL: IEEE Transactions on Reliability, Vol. R-26, No. 3, Aug. 1977.

SCOPE: System Reliability.

PROBLEM DEFINITION: The system reliability of an N-stage parallel-series system is to be determined by finding the optimal component reliability as well as the optimal number of components.

ASSUMPTIONS:

1. Each stage is in series.
2. All the stages as well as all the parallel elements used at each stage are independent.
3. All the components at each stage are simultaneously working and for a stage to fail, all its element must fail.
4. Only a single mode of failure is assumed.
5. The stage costs are additive.

SOLUTION APPROACH: The problem is formulated as a mixed integer nonlinear programming. The Hooke and Jeeves pattern search technique in combination with a heuristic approach is used to solve the problem.

COMPUTATIONAL EXPERIENCE: A solved example is given.

CONCLUSIONS: A procedure is developed to determine both the optimal component reliability as well as the optimal number of components of a system.

R-15

TITLE: OPTIMIZATION TECHNIQUES FOR SYSTEM RELIABILITY WITH REDUNDANCY - A REVIEW

AUTHOR: Tillman, F.A., Hwang, C.L. and Kuo, W.

JOURNAL: IEEE Transactions on Reliability, Vol. R-26, No. 3, Aug. 1977.

SCOPE: System Reliability.

PROBLEM DEFINITION: Optimal system reliability models with redundancy are classified by system configuration into:

1. Series
2. Parallel
3. Series-Parallel
4. Parallel-Series
5. Standby

SOLUTION APPROACH: Optimization techniques employed for system reliability with redundancy are classified into:

1. Integer Programming
2. Dynamic Programming
3. Maximum Principle
4. Linear Programming
5. Geometric Programming
6. Sequential unconstrained minimization techniques
7. Modified sequential simplex pattern search
8. Lagrange multipliers and the Kuhn-Tucker conditions
9. Generalized Lagrangian function
10. Generalized reduced gradient
11. Heuristic approach
12. Parametric approach
13. Pseudo-Boolean programming
14. Miscellaneous

CONCLUSIONS: All the optimization techniques employed in the papers surveyed have limited success in solving some small-scale system reliability optimization problems.

Few techniques have been demonstrated to be effective when applied to large-scale system reliability optimization problems.

R-16

TITLE: COMPUTER TECHNIQUE FOR ESTIMATING SYSTEM RELIABILITY

AUTHOR: Weisberg, S.A. and Schmidt, J.H.

JOURNAL: 1966 Annual Symposium on Reliability.

SCOPE: System Reliability.

PROBLEM DEFINITION: Evaluating the probability that a complex system will function in a way which permits a successful completion of a mission, and obtaining a system reliability estimate which realistically incorporates all the physical and operational features of the system.

SOLUTION APPROACH: Mathematical analysis and a computerized technique.

COMPUTATIONAL EXPERIENCE: The procedure has been mechanized by a Fortran program for the 7094 computer. The program is disucssed, and the flow charts are given. No computational results are presented. However, it was mentioned that the procedure was successful when applied to various aerospace applications. Only one numerical example was solved.

CONCLUSIONS: 1. A technique is described, which can be used to estimate the probability that a system will perform in such a way so as to allow successful completion of the mission. This technique also gives a lower bound estimate to mission success reliability, permits operational doctrine, functional degradation and functional redundancy of equipment to be incorporated into the model.

R-17

TITLE: ENHANCING TESTABILITY OF LARGE-SCALE INTEGRATED CIRCUITS VIA TEST POINTS AND ADDITIONAL LOGIC

AUTHOR: Williams, J.W. and Angell, J.B.

JOURNAL: IEEE Transactions on Computers, Vol. C-22, No. 1, January 1973.

SCOPE: LSI Circuits - Synchronous/Asynchronous.

PROBLEM DEFINITION: To study the methods of using test points in conjunction with additional logic gates to provide an easy means to set or check the state.

ASSUMPTIONS: "BRIDGING" faults result in predictable logic behavior of the network. The circuit can be set to a initial state and the final/resulting state can be checked.

Cost analysis: cost of packaging one LSI chip and cost of assembling a chip into a system are both proportional to the number of external pins.

APPROACH: Classical methods of detecting stuck-at faults in combinational and sequential circuits are discussed. "Bridging faults" are explained. It is suggested to use additional test points such that the present state can be set and read. Hence the design of the sequential circuit is so modified that 1) the circuit can easily be set to any desired internal state. 2) It is easy to find a sequence of input patterns such that the resulting output sequence will indicate whether the circuit was in a given state.

By making use of a double throw switch and a control flip-flop, circuits are modified to have a 'shift-register' mode. Based on these, a step by step procedure for testing a circuit is given.

A cost analysis model is presented and is applied to such shift register modifications. A comparison of cost between the 'test point per flip-flop' and shift register modification is considered.

COMPUTATIONAL EXPERIENCE: None

CONCLUSIONS: For most cases, (except a finite few circuits), provisions of test points are more expensive than shift-register modifications. One single test point suffices to switch the circuit to the shift-register mode, in which it is easy to set or read the state, regardless of the circuit complexity.

It is to be noted that any method of test generation for sequential circuits of LSI complexity entails large computations.

R-18

TITLE: FAULT TOLERANT SOFTWARE

AUTHOR: Hecht, Herbert

JOURNAL: IEEE Transactions on Reliability, Vol. R-23, No. 3, August 1979.

SCOPE: Sophisticated software design and coding.

PROBLEM DEFINITION: Investigation of fault tolerant techniques for applications where the consequence of failure is particularly severe.

ASSUMPTIONS: No random computer failures.

SOLUTION APPROACH: N-version programming and the recovery block approaches are considered. In the former, a number of coded programs for a given function are run simultaneously on loosely complex computers and the results compared. Wherever possible, different algorithms, languages and translations are used. In the recovery block approach, acceptance tests are used, which are devised against two criteria: To detect deviations from expected program execution or to prevent unsafe output. These result in frequent transfers to alternate routines, which take care of the situations. Further classifications of the acceptance tests are discussed. A reliability modeling is considered.

COMPUTATIONAL EXPERIENCE: Operating system software.

RESULTS AND CONCLUSIONS: Mainly used for most demanding and safety-critical applications like nuclear reactors, missiles, spaceships, etc.

R-19

TITLE: RELIABILITY MODELING AND ANALYSIS OF FAULT-TOLERANT MEMORIES

AUTHOR: Cox, G.W. and Carroll, B.D.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, No. 1, April 1978.

SCOPE: Reliability of RAM and ROM.

PROBLEM DEFINITION: Developing a memory array reliability model that can be applied to wide range of memory organizations and compute the reliability of fault-tolerant memories that employ different techniques (such as hardware redundancy, etc.) and use it to show the relative reliabilities of various memory organizations and indicate the effect of certain parameters on the predicted reliabilities.

ASSUMPTIONS: Total of 19 assumptions are assumed for different systems.

SOLUTION APPROACH: Statistical Analysis using probability distributions.

COMPUTATIONAL RESULTS: Comparisons between different models.

CONCLUSIONS:

1. Developing different reliability models for:

   a. simplex RAM
   b. an N-modular-redundant RAM
   c. a spared RAM
   d. a single error-correcting RAM
   e. a multiple-error-correcting RAM
   f. a ROM

2. Reliability characteristics of these memories are compared and it was found that memories with error-correcting capability and spare bit-planes provide the best reliability.

R-20

TITLE: TAMING THE ALL-EQUIPMENT RELIABILITY TEST

AUTHOR: Coppola, A.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, No. 1, April 1978.

SCOPE: System Reliability.

PROBLEM DEFINITION: Deriving a new empirical method for modifying the all-equipment reliability test to provide equal producer and consumer risks over a range of test lengths.

SOLUTION APPROACH: Empirical approach.

COMPUTATIONAL EXPERIENCE: The paper itself is based on computational experience from test data and experience.

CONCLUSIONS: A procedure is developed based on empirical formulas to help the user to structure an all equipment reliability test with equal risks, preventing favoring the producer or consumer, for discrimination ratios of 2.0:1, 1.5:1 or 3.0:1, as desired.

R-21

TITLE: $\overline{R}$

AUTHOR: Willoughby, Willis

JOURNAL: Quality

SCOPE: Reliable weapons.

PROBLEM DEFINITION: To provide an overview to be followed in subsequent issues of MST, based on the NEW LOOK approach.

SUMMARY: Specific concerns in acquiring reliable weapons are presented. Reliability specifications should never be in terms of numerical goals. Correcting deficiencies at a later stage works out to be expensive, so that only serious flaws are corrected, thus compromising reliability.

Most of the piece parts, though adhering to some military standards, were found faulty prior to installation in hardware. Some defects escaped their notice and entered the field.

The NEW LOOK focuses contractual and program management attention on the engineering design practices and manufacturing processes, thus achieving very good reliability. The approach recognizes the futility of waiting until just prior to production start. In fact, demonstration testing only lengthens the acquisition cycle and contributes nothing to the reliability of a system. The sensitivity of reliability for various stresses is known a priori and is made use of in NEW LOOK by setting an upper limit for these stresses. Examples of semiconductors are mentioned. The concept of 'Reliability Development Testing' is thus formed. The design should be Built-To-Print, that is, fool-proof.

Manufacturing Screening, if adopted from lower levels of assembly right through the final acceptance, results in increased reliability. NEW LOOK recommends 100% re-screening of semiconductors by the contractors using them.

The personnel are so mediocre that they hesitate to perform specific tests on working sytems, lest they cease to function.

On the panel on T & E of supportability, the author is against OT & E in the field of reliability, contending it to be too late in the program to be beneficial. Moreover, it is expensive.

SUMMARY: (Continued)

T & E should be a normal part of any engineering cycle. The independent testers should not be given the burden of doing it.

Mean logistics down time, a function of logistics is a better definition than operational availability.

Computer Aided Design (CAD) is highly praised as a marvelous tool in design.

RESULTS AND CONCLUSIONS:

NEW LOOK approach resulted in a qualitative incrase in readiness by 15%. Manufacturing screening has been proved very effective in detecting defective workmanship. For maximum effectiveness, the NEW LOOK requires adequate front end funding. This will help in reduced cost of ownership.

It is implied that most of the specifications are inadequate and do not wholly deliver what exactly is needed. Mediocre talks should be put to a stop. For the success of any project/mission, engineering commitments are a must - a commitment to do the right job, at the right time, using right methods like CAD/CAM. These do lead to real performances.

R-22

TITLE: F-16 FOLLOW-ON OPERATIONAL SUITABILITY TEST AND EVALUATION - SUBSYSTEMS EVALUATION ADDENDUM, A PHASE II, FINAL REPORT

AUTHOR: Wright, D.K., et al.

SCOPE: Military hardware subsystems. F-16 aircraft in particular.

PROBLEM DEFINITION: To perform operational tests and evaluations in accordance with AFR 80-14 and AFR 23-36 and to provide working-level details for the organizations involved.

SOLUTION APPROACH: Presents subsystem analysis from primary reliability, maintainability, availability and supportability points of view. Various subsystems such as Airframe, Crew station, Landing gear, Controls, Engine, Weapon systems, etc. are considered from operational suitability standpoint.

The operational flight program (OFP) maintainability and support software for systems like Fire control computer, Fire control radar, etc. are discussed. Adequacy of computer support resources are discussed too. The ATE function subsystem consisting of computers, switching units, Interface Test Adapters (ITA), etc. is analyzed. The display indicators, Computer/Inertial Subsystems and the Radio Frequency operations subsystems are described.

Points to be considered during upgrading of Avionics Intermediate Shop (AIS) Software are mentioned. The software maintainability and usability are analyzed and assessed on a scale of 0 to 5.

The BIT fault reporting mechanism of F-16 is briefly explained. Its general analysis, capability analysis, system maturity trends, fault analysis, diagnostic effectiveness (FI, FD and CND) are discussed.

Engineering deficiencies are considered. These are mainly contributed by radar, stores management system and missile slaving functions.

The report gives conclusions and recommendations for the various subsystems that have been analyzed. Furthermore, where relevant, a table is included of the subjective evaluation, evaluated on the basis of either excellent, satisfactory, satisfactory but needs improvement, deficient, etc. or on a 0-5 scale, with 3.3 as threshold and 4.15 as standard with 5.0 being the goal. A repair time analysis is included.

RESULTS AND CONCLUSIONS: This addendum consists of conclusions and recommendations of the various hardware units and software aspects of the F-16 aircraft. Furthermore, each subsystem is subjectively evaluated wherever necessary.

A set of points to be considered during ATE acquisitions or upgrading are aptly included.

R-23

TITLE: EFFECTIVENESS OF U.S. FORCES CAN BE INCREASED THROUGH IMPROVED WEAPON SYSTEM DESIGN -- A REPORT TO THE CONGRESS

AUTHOR: Controller General -- GAO PSAD 81-17

SCOPE: Weapon Systems.

PROBLEM DEFINITION: To study the influence of logistic support, human factors and quality assurance on the effectiveness of weapon system design - in order to identify the cause of problems and to recommend meaningful actions to reduce these.

The concept of logistic support, human factors and quality assurance are briefly described. The DoD views on these, and additional considerations needed are mentioned. The factors contributing to the ownership considerations are listed. Weapon systems were selected for review based on problems that

- could have been anticipated during acquisition cycle
- were missions significant
- were experienced commonly
- had enough data on acquisition process decision

Problems experienced by major systems are mentioned as an appendix.

Each of the three - logistic support, human factors and quality assurance are considered separately and based on these analyses. Various recommendations are made to the congress, such as

- to modify the current data reporting procedures.
- to establish logistic support research.
- to provide for improved testing and evaluation.
- to modify the existing specifications and standards on human factors.
- to produce comprehensive guidance as to how designs are to be evaluated for quality assurance.

Relevant GAO reports issued between January 1979 and November 1980 are listed.

It is inferred from the reply by OSD that OSD too has totally recognized the problems and is taking immediate action, making necessary changes and reviewing certain military standards.

PROBLEM DEFINITION (Continued)

Anticipation and elimination of problems during the design and acquisition stages are highly recommended.

RESULTS AND CONCLUSIONS: Long gestation period in weapon development can be avoided, achieving technological excellence -- not by increased complexity, but by anticipating shifts in military requirements. Over reliance on technology should be stopped. It is recommended that the congress direct more attention to DoD's budget to such ownership consideratons.

From this issue, the following points can be concluded:

*The complexity/sophistication of the system designed should bear in mind the user who operates it.

*Too much automation is not advisable, leading to increased number of black boxes.

*Non performance of weapon system is attributed mainly to unreliable designs.

*Human reliability, if not properly considered can result in increased errors in operation and maintenance, and can lead to very serious problems.

*The specifications/standards should include limitations on human skill levels.

*Manpower and personnel needs are to be forecasted well in advance.

*50% of all weapon system failures have been traced to human ineptitude or poor human reliability.

*The reliability intended to be designed into a system is often not being achieved in the field.

*Worst case design (pessimistic approach) should be stressed.

*Lack of design evaluation guidance and incomplete policy implementation along with additional and better qualified staffing is necessary.

*Most of the problems experienced can be tracked back to the extent of ownership considerations in the early acquisition process.

R-24

TITLE: APPLICATION OF PATTERN RECOGNITION TO FAILURE ANALYSIS AND DIAGNOSIS

AUTHOR: Pau, L.F.

JOURNAL: Human Detection and Diagnosis of System Failures (1980), Ruskilde, Denmark

SCOPE: Review.

SUMMARY: Basic concepts of failure analysis and diagnosis are discussed that include: failure, degradation, failure mode, failure detection, failure localization, failure diagnosis, analysis and monitoring. Then, the effects of failure analysis and diagnosis on the system reliability and survivability are discussed. Errors of the diagnostic system are explained. They are incorrect diagnosis, false alarm, and missing a failure.

Application of pattern recognition to failure diagnosis and performance monitoring is then considered. Four problems are examined: pattern measurement, learning, feature extraction and classification. For each problem, the specific aspects met in applying pattern recognition to failure analysis and diagnosis and the pattern recognition methods used are reviewed. Finally, the publications describing some major implementation are surveyed.

R-25

TITLE: TESTING AND DIAGNOSIS OF LOGIC

AUTHOR: McCluskey, E.J.

JOURNAL: EURO IFIP 79

SCOPE: A survey of techniques for testing and improving testability.

PROBLEM DEFINITION: The tradition of designing digital systems without attention to the fact that they will have to be maintained is no longer cost-effective.

SUMMARY: When comparing testing techniques coverage, cost, and storage requirements must be considered. Testing techniques include complete enumeration, minimum length tests and compact tests (minimum storage tests based on random numbers).

At the design stage a measure of testability has been defined which is in terms of the controllability and observability of the links in the circuit.

Also discussed are techniques for test point insertion, testing by shift register scan, signature analysis, and self testing by duplication of circuitry.

S - SEMIAUTOMATIC AND MANUAL TEST PROCEDURES

S-1 Allen, D.J. and Rao, M.S. Madhava, "New Algorithms for the Synthesis and Analysis of Fault Trees," Industrial Engineering Chemical Fundamental, Vol. 19 (1980).

S-2 Barsi, F., Grandoni, F. and Maestrini, P., "A Theory of Diagnosability of Digital Systems" IEEE Transactions on Computers, Vol. C-25 (1976).

S-3 Brule, J.D.; Johnson, R.A. and Kletsky, E.J., "Diagnosis of Equipment Failures," IRE Transactions on Reliability and Quality Control, Vol. RQC-9 (1960).

S-4 Butterworth, R., "Some Reliability Fault Testing Models," Operations Research, Vol. 20 (1972).

S-5 Chang, H.Y., "An Algorithm for Selecting an Optimum Set of Diagnostic Tests," IEEE Transactions on Electronic Computers, Vol. EC-14 (1965).

S-6 Cohn, M. and Ott, G., "Design of Adaptive Procedures for Fault Detection and Isolation," IEEE Transactions on Reliability, Vol. R-20 (1971).

S-7 Ben-dov, Y., "Optimal Testing Procedures for Coherent Systems," AD-A057952 (1977).

S-8 Gluss, B., "An Optimum Policy for Detecting a Fault in a Complex System," Operations Research, Vol. 7 (1959).

S-9 Halpern, J., "A Sequential Testing Procedure for a System's State Identification," IEEE Transactions on Reliability, Vol. R-23 (1974).

S-10 Johnson, R.A., "An Information Theory Approach to Diagnosis," 6th Symposium on Reliability and Quality Control (1960).

S-11 Kletsky, E.J., "Diagnosis of Equipment Failures," RADC-TR-60-67B Final Technical Report, Part I/II (1960).

S-12 Kletsky, E.J., "An Application of the Information Theory Approach to Failure Diagnosis," IRE Transactions on Reliability and Quality Control, Vol. RQC-9 (1960).

S-13 Mayeda, W. and Ramamoorthy, C.V., "Distinguishability Criteria in Oriented Graphs and Their Application to Computer Diagnosis-I," IEEE Transactions on Circuit Theory, Vol. CT-16 (1969).

S-14 Merrill, H.M., "Failure Diagnosis Using Quadratic Programming," IEEE Transactions on Reliability, Vol. R-22 (1973).

S-15 Nakano, H., "Internal Test Terminals for System Diagnosis," Electronics and Communication in Japan, Vol. 54-C (1971).

S-16 Nakano, H. and Nakanishi, Y., "A Procedure of Determining Test Terminals for System Diagnosis," Systems* Computers* Controls, Vol. 2 (1971).

S-17 Nakano, H. and Nakanishi, Y., "Necessary and Sufficient Conditions for 1-Distinguishability in System Diagnosis," Systems* Computers* Controls, Vol. 3 (1972).

S-18 Scola, P.J., "TOLTS, Total On-Line Testing Systems", Honeywell Information Systems, Inc., Index Serial #1084.

S-19 Seshu, S., and Freeman, D.N., "The Diagnosis of Asynchronous Sequential Switching Systems," IRE Transactions on Electronic Computers, Vol. EC-11 (1962).

S-20 Seshu, S., "On An Improved Diagnosis Program", IEEE Transactions on Electronic Computers, Vol. EC-14, (1965).

S-21 Seshu, S., "Self Repairing Machines". Final Report - Part 2/2 RADC-TR-61-91B, (1961).

S-22 Winter, B.B., "Optimal Diagnostic Procedures", IRE Transactions on Reliability and Quality Control, Vol. RQC-9 (1960).

S-23 Genet, R.M., "An Introduction to the Theory and Improvement of Multi-level Tests in Repair Processes", Plans and Management Staff Office Aerospace Guidance and Metrology Center Newark Air Force Station, Newark, Ohio 43055 (1972).

S-24 Levy, Girard W. et al., "Final Report on Improved Maintenance Procedures for Inertial Guidance Systems". PRAM Program Office, AFSC, Aeronautical Systems Division: Wright-Patterson AFB (1976).

S-25 Bogard, D.R. et al., "Operation and Support Cost Characteristics of Testers and Test Subsystems". RADC-TR-79-334, Final Technical Report (1980).

S-1

TITLE: New Algorithms for the Synthesis and Analysis of Fault Trees.

AUTHOR: Allen, David J. and Rao, M.S. Madhava

JOURNAL: Industrial Engineering Chemical Fundamental, Vol. 19, No. 1, 1980.

SCOPE: Analysis and synthesis of fault trees.

PROBLEM DEFINITION: Proposing new algorithms for the synthesis and analysis of fault trees to facilitate fault tree analysis and allow the analyst to focus his attention upon the system's behavior.

SOLUTION APPROACH: Graph theory.

COMPUTATIONAL EXPERIENCE: The proposed techniques have been used in the preparation and analysis of fault trees in the failure analysis of a chemically active, fluidized bed demonstration unit. The analysis resulted in the synthesis of several fault trees, one containing 500 gates. Synthesis from the diagraph of this largest tree and its subsequent analysis into minimal out sets containing up to 4 elements required 30 seconds of CPU time on a CDC 6600 computer.

CONCLUSIONS: Two computer programs and their algorithms are described:

1) An algorithm and program for fault tree synthesis that allows the analyst to concentrate upon the task of system definition.

2) A fault tree analysis program that is significantly faster than programs currently in use when applied to large, complex fault trees.

S-2

TITLE: A Theory of Diagnosability of Digital Systems.

AUTHOR: Barsi, Ferruccio; Grandoni, Fabrizio; and Maestrini, Piero.

JOURNAL: IEEE Transactions on Computers, Vol. C-25, No. 6, June 1976.

SCOPE: Automatic fault diagnosis of systems decomposed as a number of interconnected units.

PROBLEM DEFINITION: To develop necessary and sufficient conditions for t-diagnosability in both cases of one-step diagnosis and diagnosis with repair. The problem of optimal assignment of testing links in order to achieve a given diagnosability is also considered and classes of optimal t-diagnosable systems are presented for arbitrary values of t in cases of one step diagnosis and diagnosis with repair. If one application of the set of tests is sufficient to identify all faulty units, one-step diagnosis is said to occur. A diagnostic process allowing identification of at least one faulty unit is called diagnosis with repair.

ASSUMPTIONS:

1. Each test is operated by a single unit.
2. Each unit has the capability to test any other unit except itself.
3. The testing unit is assumed fault free.
4. Any unit performs at most one test on any other unit.

APPROACH: Graph theory is used to prove twelve theorems on diagnosability.

COMPUTATIONAL EXPERIENCE: None

S-3

TITLE: Diagnosis of Equipment Failures.

AUTHOR: Brule, J.D.; Johnson, R.A. and Kletsky, E.J.

JOURNAL: IRE Transactions on Reliability and Control, Vol. RQC-9, April, 1960.

SCOPE: Modeling of equipment and test procedures.

PROBLEM DEFINITION: Terminology and procedures for finding an optimum testing procedure for some special cases are developed.

SOLUTION APPROACH: Any equipment can be broken down into its functional elements for purpose of modeling. The equipment is assumed to have no feedback or redundancy.

A test will cause an evaluation of each element as either good, bad, or questionable. A given test will pass if the elements being tested are all good, and fail otherwise. A test may be represented by a binary N-vector where N is the number of elements in the equipment. A "1" in the i^{th} position in the vector denotes that the i^{th} element is not tested. A "0" means that the i^{th} element must be good for the test to pass.

In combinational testing the next test to be performed is independent of all previous tests. However, sequential testing takes advantage of prior testing results to provide faster isolation of the faulty element.

An assumption often made is that exactly one element is faulty. This yields a simplified sequential testing diagram. For cases where all of the $2^{N-1} - 1$ tests are not possible a method for determining if the available tests will be adequate is given.

When assumptions are relaxed to allow the equipment to be faultless or allow for multiple faults, this can be handled using techniques developed for the single fault case.

The problem of developing optimum diagnostic procedures can be based on several criteria including average cost and min-max.

Procedures for developing optimum diagnostics are given for the case of equal cost, equal or unequal probabilities.

CONCLUSIONS: It is believed that the concepts and techniques developed here are applicable to the diagnostic procedures for a wide class of equipment.

S-4

TITLE: Some Reliability Fault Testing Models.

AUTHOR: Butterworth, Richard.

JOURNAL: Operation Research, Vol. 20, March 1972

SCOPE: Fault Testing Models - Secondary Isolation

PROBLEM DEFINITION: A system is composed of n components. The system works if k or more of its components work (k/n type). The problem is to find feasible test procedures to locate the failed component and find a feasible testing procedure to determine the state of the system.

ASSUMPTION: The components are assumed to function or fail independently.

SOLUTION APPROACH: Mathematical Models.

COMPUTATIONAL EXPERIENCE: None.

CONCLUSIONS: Several models are presented. In the first model a feasible test procedure to determine if the system is working or has failed is developed. This is solved for the series and parallel systems and under a certain condition for the general k/n system.

In another model, a feasible test procedure is derived to locate all failed components for the general k/n system.

S-5

TITLE: An Algorithm for Selecting an Optimum Set of Diagnostic Tests.

AUTHOR: Chang, Herbert Y.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-14, No. 5, Oct. 1965.

SCOPE: Combinational diagnostic tests for large digital systems.

PROBLEM DEFINITION: To provide an algorithm for selecting a good (locally optimized) set of diagnostic tests which contains no redundancy.

ASSUMPTIONS: Assume there are n faults, f_1, $f_2,\ldots,f_n$ which can exist in a system, one at a time. Any time a fault occurs, a set of m tests t_1, $t_2,\ldots,t_m$ is applied and results observed. The test results can be recorded in binary; "1" means the corresponding test has failed and a "0" indicates the test passed. The data matrix $D = [d_{ij}]_{n,m}$ has one row for every fault $f_i(1\leq i\leq n)$ and a column for every test $t_j(1\leq j\leq m)$. Thus d_{ij} is "1" if fault f_i is detected by test t_j and "0" if not. Rows of D are called fault patterns and columns are called test patterns. A set of patterns is said to form an equivalent set if no two patterns in the set are distinguishable. Two fault patterns

$f_i = [d_{i1}d_{i2}\ldots d_{im}]$ and $f_j = [d_{j1}d_{j2}\ldots d_{jm}]$ are distinguishable if $d_{ik} \neq d_{jk}$ for some k. Diagnostic tests are redundant if they can be eliminated from the data matrix without producing additional indistinguishable fault patterns.

APPROACH: A branch matrix $D[t_{i1}{}^{e1}t_{i2}{}^{e2},\ldots,t_{is}{}^{es}]$ is a submatrix of data matrix D whose columns are all columns of D permuted in the order $t_{i1},t_{i2},\ldots,t_{is},\ldots,t_m$, and whose rows are all those which share a common pattern $e_1e_2,\ldots e_s$ associated with tests $t_{i1}t_{i2},\ldots,t_{is}$ where s is the number of selected tests.

$D[t_{i1}^{e1}, t_{i2}^{e2}, \ldots t_{is}^{es}]$ can also be written as $De[t_{i1},t_{i2},\ldots,t_{is}]$ where e is the decimal equivalent of $e_1e_2,\ldots, e_s$ in binary.

The weight of a test may be regarded as a means for comparing the relative importance of tests. Using the

APPROACH (Continued)

notion of test weighting and branch matrices an iterative algorithm is presented to select a locally optimum set of diagnostic tests from a data matrix.

CONCLUSIONS:

The process terminates in a finite number of iterations. In the worst case this will be min (m,n) iterations. The process is described as simple, straightforward, and programmable. The algorithm will in general tend to give a "fairly good" set of test patterns, but is not guaranteed to be absolutely minimal. An overall optimization scheme is desirable but seems impractical.

S-6

TITLE: Design of Adaptive Procedures for Fault Detection and Isolation.

AUTHOR: Cohn, Martin and Ott, Gene.

JOURNAL: IEEE Transactions on Reliability, Vol. R-20, No. 1, Feb. 1971.

SCOPE: Design of testing procedures.

PROBLEM: To design an adaptive testing procedure that detects a failure and isolates the faulty component while minimizing the expected cost of testing.

ASSUMPTIONS: 1) The system is assumed to be a collection of elements, 2) a fault is any anomaly in the input-output behavior of an element, 3) a priori probabilities of element failures can be accurately estimated, 4) probabilities of multiple failures are negligible.

APPROACH: A test tree is a decoding tree at each node of which a received 0 or 1 may be construed as passage or failure of a test, directing the decoder to branch left or right to the next node. In addition to the n elements of the system, an (n + 1) st dummy element denotes the condition "no fault". If to every possible ambiguity subset there can be assigned an evaluation, consisting of the least expected cost of resolving that ambiguity, then the evaluation of the subset of complete ignorance is the cost of the optimal tree. The evaluation of a subset is simply the minimum, over all partitionings, of the expected cost of the test plus the evaluations of the two subsets thus reached. Recursion continues until all subsets are single elements so no ambiguity exists.

COMPUTATIONAL EXPERIENCE: Fault isolation will require about 2^n memory locations and about $1/2(3^n)$ computations.

S-7

TITLE: Optimal Testing Procedures for Coherent Systems

AUTHOR: Ben-Dov, Y.

JOURNAL: AD-A057 952, Sept., 1977.

SCOPE: Optimal testing procedures.

PROBLEM DEFINITION: A system is composed of n components that either work or fail. Associated with each component is a cost for testing, and an a priori probability that it is functioning. The problem is to find the optimal testing policy which minimizes the expected cost of testing this system.

ASSUMPTIONS: Components function or fail independently of each other.

SOLUTION APPROACH: Branch and Bound algorithm.

COMPUTATIONAL EXPERIENCE: A solved example is presented to explain the algorithm.

CONCLUSIONS: The concept of the importance of components is used to develop a branch and bound algorithm which determines the optimal testing policy for any coherent system.

S-8

TITLE: An Optimum Policy for Detecting a Fault In a Complex System.

AUTHOR: Gluss, Brian.

JOURNAL: Operations Reseach, Vol. 7, 1959.

SCOPE: Fault testing models - secondary isolation.

PROBLEM DEFINITION: A system consists of N modules. Each module contains a number of items or subcircuits. If a faulty module has been determined, it is required to dictate a search stategy that will minimize the associated expected cost.

ASSUMPTIONS: In model I, overall tests of each module may be performed. In model II, overall module tests are not possible, and penalty costs must be paid whenever the search moves from one module to another.

APPROACH: Mathematical Models.

COMPUTATIONAL EXPERIENCE: Only one solved example.

CONCLUSIONS: Two models are presented. Equations are developed for both, but only optimum search strategy is derived for the first model to find the failed unit in the known predetermined module.

S-9

TITLE: A Sequential Testing Procedure for a System's State Identification.

AUTHOR: Halpern, Jonathan.

JOURNAL: IEEE Transactions on Reliability, Vol. R-23, No. 4, Oct. 1974.

SCOPE: An adaptive testing procedure for determining the state of the system.

PROBLEM DEFINITION: In the case where a system is entirely or partially consumed upon use, one wishes to know the system's state without actually operating the system. Based on that need, an adaptive testing procedure for determining the state of the system is developed.

ASSUMPTIONS: The system is assumed to be coherent and irreducible.

APPROACH: The solution is based on the minimal paths and minimal cuts of the system. An important and desirable feature of this procedure is that it does not require the complicated construction of a tree as do the usual procedures.

COMPUTATIONAL EXPERIENCE: The procedure is demonstrated for a 5-component system.

CONCLUSIONS: The sequential testing procedure presented is shown to be an optimal policy for series-parallel and k-out-of-n: G systems. It is also argued, without proof, that this procedure will be optimal for many other systems.

S-10

TITLE: An Information Theory Approach to Diagnosis

AUTHOR: Johnson, Richard A.

JOURNAL: 6th Symposium on Reliability and Quality Control, 1960.

SCOPE: Sequential test procedures.

PROBLEM: To develop a simple systematic approach to constructing efficient and inexpensive test procedures.

APPROACH: The term "information" as used in information theory is a quantitative measure of the amount of uncertainty or ambiguity as to which of several specific events of a priori probability Pj will occur. The uncertainty or ambiguity at the initial state is given by $A_o = -\sum_j pj \log pj$. The average amount of ambiguity removed by each test can be expressed as the difference between the ambiguity associated with each of the two succeeding states weighted with the probability of occurrence. So the average ambiguity removed by test T_k is $A_k = A_x - [PA_y + (1-P)A_z]$.

This may also be expressed as

$$A_k = -P \log P - (1-P) \log (1-P)$$

Since it is desirable to remove as much ambiguity as possible for the least cost, the figure of merit associated with test k of cost C_k is $F_k = A_k/C_k$.

The testing sequence is determined by evaluating F_k for each test at the initial state and performing the test having the largest F_k. This procedure is repeated for the two states reachable from that test.

COMPUTATIONAL EXPERIENCE: This approach yields a low but not guaranteed minimum cost testing procedure. Several cases where minimum cost is obtainable are used to compare the information theory approach cost and the true minimum cost. Usually the average costs obtained are equal to or only slightly greater than the minimum possible values. When the cost of a group of tests depends on the sequence in which they are performed, the information theory figure of merit is thus the only feasible approach to determining inexpensive test procedures.

S-11

TITLE: Diagnosis of Equipment Failures

AUTHOR: Kletsky, Earl J.

JOURNAL: RADC - TR - 60-67B, Final Report - Part II of II, April, 1960.

SCOPE: Any system in general, electronic systems in particular.

PROBLEM DEFINITION: To apply information theory toward diagnosis of electronic systems and to computerize the diagnostic procedures.

SOLUTION APPROACH: A R-27B B/GR receiver is chosen for study. A figure of merit

$F_k = \frac{\bar{A}k}{c_k}$ is defined, based on average ambiguity removed by a test and the cost of performing it. The test which maximizes F_k is chosen.

The technique involved is summarized under 4 major steps:

1. Formulation of tests and unit operations.
2. Accumulation of unit operation costs.
3. Determination of a priori failure probabilities for elements.
4. Application of the figure of merit.

A diagnostic chart, capable of localizing faults to a particular section is attached. The process should always begin from the first step. A scheme for a hypothetical aircraft fire control system is given to show generality of the approach.

COMPUTATIONAL EXPERIENCE: A program written specifically for IBM-650 Magnetic Drum Computer was developed. A master flow diagram is listed. Each of the boxes in it are described sufficiently. Some of them are further expanded.

CONCLUSIONS: The diagnostic procedure can also be used for check-out procedure by performing a sum set of tests. A sample of the computer output is attached - (for the case of $\leq$10 elements and $\leq$100 tests).

For practical cases (>>10 elements, >>100 tests), additional external storage is needed but the same logical structure remains. In this approach, accurate failure probabilities aren't needed. Availability of failure symptoms effectively alter the a priori probability of failure of functional elements. In case of monitored systems, a group of out-of-tolerance signals

CONCLUSIONS (Continued)

can be used to initiate a set of pre-programmed diagnostic procedures.

Most suitable for:

1. Self monitoring systems.
2. New system design with strong consideration toward efficient failure diagnostics.
3. Ease of maintenance of existing operational systems - even by technicians with minimal fundamental electronics.

S-12

TITLE: An Application of the Information Theory Approach to Failure Diagnosis.

AUTHOR: Kletsky, E.J.

JOURNAL: IRE Transactions on Reliability and Quality Control, December, 1960.

SCOPE: Any electronic systems (analog or digital), monitored systems, new system design.

PROBLEM DEFINITION: To demonstrate by means of a practical example, the validity of the technique based on information theory.

CONSTRAINTS/ ASSUMPTIONS: A priori probability that the next test will pass based on the outcome of the present test is necessary.

SOLUTION APPROACH: A detailed example to demonstrate the above technique is discussed. The feasibility of the approach is shown. The procedure to be used in its implementation is outlined in detail. A figure of merit is the ratio of ambiguity removed by a test to the cost of performing the test.

$$F_k = \frac{-P \log_2 P - (1-P) \log_2 P}{C_k}$$

C_k = cost of performing the test

P = probability that the test will pass

The example of a standard Air Force communications receiver (R-278 B/GR) is analyzed, and a diagnostic procedure prepared. A priori probability of failure is found by using the failure rate. Using this, the probability with which a given test passes is tabulated. A detailed testing diagram is attached on the basis of the outcome of present test. The chart indicates the next sequence of tests to be applied.

COMPUTATIONAL EXPERIENCE: A program has been written for the basic IBM-650 magnetic drum computer. Features of the program are enclosed.

CONCLUSIONS: Manufacturer's reliability specification are important in arriving at the failure probability. Events prior to the failure (symptoms) help a great deal in arriving at the fault faster. Such symptoms alter the a priori probability of failure of the components. If these are taken care in the inital design stages, then a very efficient failure diagnosis can be obtained.

S-13

TITLE: Distinguishability Criteria in Oriented Graphs and Their Application to Computer Diagnosis - I.

AUTHOR: Mayeda, W. and Ramamoorthy, C.V.

JOURNAL: IEEE Transactions on Circuit Theory, Vol. CT-16, No. 4, Nov. 1969.

SCOPE: Fault diagnosis in a sequential system.

PROBLEM DEFINITION: Using a directed graph to represent a system in which a signal is transmitted by edges in the direction of their orientation. The vertex is considered as a relay station such that if the vertices are properly operating (fault free), the output signal will be error-free (good) and vice versa. Thus by injecting proper test patterns at selected test points and monitoring the resulting output at other test points we can determine whether or not all the vertices accessed by these input test patterns are operating properly.

SOLUTION APPROACH: Graph theory.

COMPUTATIONAL EXPERIENCE: Solved examples.

CONCLUSIONS: Distinguishability criteria in directed graphs are developed and bounds are derived on the number of test points needed to locate faults in a sequential system. Also a necessary and sufficient condition for 1 distinguishability of a SEC (single entry - single exit connected) graph is developed.

S-14

TITLE: Failure Diagnosis Using Quadratic Programming.

AUTHOR: Merrill, Hyde M.

JOURNAL: IEEE Transactions on Reliability, Vol. R-22, No. 4, Oct. 73.

SCOPE: Fault diagnosis in complex systems.

PROBLEM DEFINITION: A system becomes inoperative due to the failure of one or a few components. Based on a limited set of measurements it is necessary to determine which component failed.

SOLUTION APPROACHES:

1. Psuedoinverse method.
2. Pattern recognition approach.
3. Quadratic programming approach.

COMPUTATIONAL EXPERIENCE: The quadratic programming algorithm has been tested on a mathematical model of a high performance inertial guidance system. The algorithm correctly identified all failed parameters and computed their values with errors of less than 1%. The quadratic algorithm is much faster than the pattern recognition algorithm. It also requires a small number of pivots on a fairly large matrix.

CONCLUSIONS: Three mathematical formulations are presented:

1. The first is solved using the pseudoinverse and yields diagnoses that are not realistic.
2. The second formulation solved by a pattern recognition search yields reasonable results but generally requires excessive computer time.
3. The third is solved by a quadratic programming algorithm. The convergence of the algorithm is proved.

S-15

TITLE: Internal Test Terminals for Systems Diagnosis.

AUTHOR: Nakano, Hideo.

JOURNAL: Electronics and Communication in Japan, Vol. 54-C, #12, 1971.

SCOPE: Internal test terminals required for diagnosis and their relation to the structure of a graph.

PROBLEM DEFINITION: To determine a set of internal test terminals using distinguishability criteria.

CONSTRAINTS/
ASSUMPTIONS:

1. Normal unit should produce normal output as a response to normal input
2. A failed or abnormal unit responds abnormally.
3. A unit produces output only when input is present.

SOLUTION APPROACH: A diagnosis table T of output patterns according to the failure patterns of the system is constructed, which is then used to determine the internal test terminals. Even the reachability matrix of nodes could be used to arrive at such conclusions. Both methods are outlined with an example. Hasse graphs are defined with their applications. SPASEC graphs are discussed.

A graph theory approach is used.

Sufficient theory is outlined and proved to arrive at final conclusions.

CONCLUSIONS: The theory concludes that a system that has SPASEC graph as its functional model has a unique set of internal test terminals. The one-distinguishability of system failures is considered and an efficient method for determining a set of internal test terminals via the Hasse graph is presented. A study of system-diagnosis graphs that possess unique sets of internal terminals might play some role in providing structures of functional independence.

S-16

TITLE: A Procedure of Determining Test Terminals for System Diagnosis.

AUTHOR: Nakano, H., and Nakanishi, Y.

JOURNAL: Systems* Computers* Controls, Vol. 2, No. 5, 1971.

SCOPE: Minimal fault diagnostic test

PROBLEM DEFINITION: Determining the terminal test which has the minimum number of elements among terminal tests for system diagnosis.

ASSUMPTION: The probability of simultaneous failure of two or more units is so small as to be negligible.

SOLUTION APPROACH: Graph-theoretic approach.

COMPUTATIONAL EXPERIENCE: A flow chart for the proposed algorithm is presented. However no examples or computational results are presented.

CONCLUSIONS:

1. A method has been proposed by which internal test terminals are determined that can compose a fault diagnosis test and definitely locate the fault unit.

2. It is shown that the properties of the upper directed cutset of an acyclic SEC graph can be particularly useful in system diagnosis.

3. An estimate is derived of the lower bound on the number of internal test terminals needed for system diagnosis.

S-17

TITLE: Necessary and Sufficient Conditions for 1-Distinguishability in System Diagnosis.

AUTHOR: Nakano, H. and Nakanishi, Y.

JOURNAL: Systems* Computers* Controls, Vol. 3, No. 5, 1972.

SCOPE: Minimal Fault Diagnostic Test

PROBLEM DEFINITION: Discussing necessary and sufficient conditions for 1-distinguishability in system diagnosis, determining test terminals sets, and modifying two previous papers published by the same authors.

SOLUTION APPROACH: Graph theory.

COMPUTATIONAL EXPERIENCE: Only three examples were solved.

CONCLUSIONS:

1. The necessary and sufficient conditions for 1-distinguishability are derived.
2. Two previous papers of the same authors are reexamined and modified.

S-18

TITLE: TOLTS, Total On-Line Testing System

AUTHOR: Scola, P.J.

JOURNAL: Index Serial #1084, Honeywell Information Systems, Inc.

SCOPE: Digital Systems and Computers

PROBLEM DEFINITION: To run diagnostics on a machine when it is ON LINE - to increase MTFB, using TOLTS, MOLTS, ROLTS, COLTS, POLTS. To optimize user efficiency.

ASSUMPTION: The complete testing sequence is resident in the memory.

APPROACH: TOLTS is sub-classified into 4 other systems. (Main frame, remote, communication, peripheral - OLTS). Each subsystem has a specific application. A common memory layout for the subsystems is listed. Same common principles apply to the coding in the operating systems - for characters and mnemonics. A brief description of each subsystem is given.

COMPUTATIONAL EXPERIENCE: OPTS-600 (on line peripheral test system) is mentioned.

CONCLUSIONS: Benefits of TOLTS are listed. A big advantage is that the tests are executed in the same environment as the user programs. Specific advantages of each subsystem are mentioned.

The command structure allows addition of new commands - flexibility. A large scale multiprogramming/ processing systems can be maintained with minimal off-line maintenance.

S-19

TITLE: The Diagnosis of Asynchronous Sequential Switching Systems.

AUTHOR: Seshu, S. and Freeman, D.N.

JOURNAL: IRE Transactions on Electronic Computers, Vol. EC-11, No. 4, Aug., 1962.

SCOPE: Sequential switching circuits.

PROBLEM DEFINITION: To develop a testing procedure for a sequential switching circuit using a program generated by an IBM 7090 computer, based on the logical description of the circuit to be tested.

ASSUMPTIONS/ CONSTRAINTS: Nonclocked sequential circuits are considered, are concerned with failure of logical elements only.

SOLUTION APPROACH: The results of each test are used as a basis for deciding on the next test to be performed.
The criteria for acceptable tests are laid out. A possible N faults in the machine makes it behave as though it were N+1 machines (including the good one). The procedure simulates each of the N+1 possible machines based on the outcome of tests. The machines are partitioned into equivalence classes - one for each distinct output configuration. This is done for all the tests until all the classes are partitioned as far as possible.
The options/features of the 7090 program are discussed. An example is worked out to illustrate the procedure.

COMPUTATIONAL EXPERIENCE: The 7090 program organization is shown. The features of the program are explained.

CONCLUSIONS: Fewer tests are required to identify a failure. A simple example is illustrated and the outputs are tabulated to explain the results.

No look up table is needed. Two major problems left to be tackled are to generate good reset memory states and first inputs. Significantly, for a strongly sequential circuit, the program is very efficient.

S-20

TITLE: On An Improved Diagnosis Program.

AUTHOR: Seshu, Sundaram.

JOURNAL: IEEE Transactions on Electronic Computers, Vol. EC-14, No. 1, Feb. 1965.

SCOPE: Sequential Circuits.

PROBLEM: To study CSX-1 computer from point of view of self diagnosis and examine the problems that arise.

ASSUMPTIONS:

1. The class of possible failures is known and finite.
2. Each failure transforms a sequential circuit into another sequential circuit, i.e. only logical failures are considered.
3. Even under failure conditions, it is possible to reset the feedback lines.

APPROACH: The CDC 1604 program is explained. It has 2 drive routines.

1. Straightforward simulation driver - simulates any given sequence of inputs.
2. Normal diagnosis driver - makes a simple minded indistinguishability test on each subset before proceeding on any of the 4 strategies
   a) Best next or return to good input strategy - the most useful.
   b) Try wandering - based on a fixed number of psuedo-random steps in the hope of searching a useful input.
   c) Combinational strategy - treats the circuits as combinational.
   d) Reset strategy - all available resets are stored in the memory. The strategy tries each of the resets to see if any useful information is obtainable. Two criteria are used to compute the figure of merit of a test.

1. Information gain

   $I = - (\Sigma p_j \log \Sigma p_j + \Sigma q_j \log \Sigma q_j)$

2. Check out or detection criterion =

$$\frac{\text{Number of machines eliminated}}{\text{Original number in subset}}$$

Concepts of simulation technique are explained in detail.

COMPUTATIONAL EXPERIENCE: The CDC 1604 program is used. Its routines are similar to the CDC fortran resident.

CONCLUSIONS: CDC 1604 program was better than IBM 7090 program in the sense of flexibility. It is compared to the other existing programs at that time and the merits/demerits listed. Some of its flaws have been pointed out. Owing to its flexibility it is possible to join manually generated lists to program generated tests.

S-21

TITLE: Self Repairing Machines.

AUTHOR: Seshu, Sundaram.

JOURNAL: Final Report, Part 2/2, RADC - TR - 61-91B, April 1961.

SCOPE: Electronic Systems - digital.

PROBLEM DEFINITION: For any system, to provide a test equipment that can diagnose the system and maintain it such that the mean life of the system is 10 to 100 times that of an unmaintained system.

ASSUMPTIONS: The class of failures which can occur is known; every failure results in a change in the basic logic (1 or 0 and not in between). it is possible to reset the machine even under failure conditions - to a known initial state.

APPROACH: The tests are chosen to satisfy the following conditions -

1. The tests can follow each other.
2. The tests are so chosen that the machine is well behaved to that input.

The computations are aided by simulating N+1 machines on a computer. Races and oscillations are taken care of. Each test partitions the machines into a smaller set. The next choice of the test is suitably made based on the results on the previous test. The sequence is terminated when the subset is sufficiently small to be replaced by new elements. The method of choosing a test is explained.

COMPUTATIONAL EXPERIENCE: The LGP-30 computer was used. Organization of the program is given.

CONCLUSIONS: Eight examples are considered and their diagnosis explained in detail. The complexity of the testing for each of the examples above are summarized in a table.

"And-or-invert" logic is preferable from diagnosis point of view. The feedback lines must be accessible both for resetting and for observation. Interstate transitions of more than two steps are to be avoided. To obtain complete diagnosis, we have to work back and forth between simulation diagnosis and design.

S-22

TITLE: Optimal Diagnostic Procedures

AUTHOR: Winter, B.B.

JOURNAL: IRE Transactions on Reliability and Quality Control, Vol. RQC-9, No. 3, December, 1960.

SCOPE: Multilevel equipment - for single faults/failures.

PROBLEM DEFINITION: To obtain an optimum diagnostic procedure in the sense of minimizing expected cost.

CONSTRAINTS/ ASSUMPTIONS: Test either one element at a time or all at once. Cost is linear. If a test isn't performed, its cost is zero. A priori probability of failure is known.

APPROACH: If one or more elements are bad, a method is described for the testing sequence, until the fault is located. Analysis for single element failure is included - for a multilevel equipment.
Exponential failure distributions are made use of in the analysis.

CONCLUSIONS: An example with five elements and one failure is considered. On failure, the sequence of elements to be tested is specified. It is not possible to generalize for large networks which need lots of tests. The principle of cost factor is useful in determining the sequence of tests to be applied.

S-23

TITLE: An Introduction to the Theory and Improvement of Multi-Level Tests in Repair Processes.

AUTHOR: Genet, Russell M.

JOURNAL: Plans and Management Staff Office Aerospace Guidance and Metrology Center Newark Air Force Station; Newark, Ohio 43055, 20 June 1972.

SCOPE: Improvement of testing based on field performance.

OBJECTIVE: The goal was to develop a program to improve fault detection/isolation tests in the post-deployment stage.

ASSUMPTIONS: Systems considered have at least two subsystems.

SUMMARY: The essence of a test is (1) to make measurements, (2) to sort items based on these values, and (3) to do something different with the items in each category (measurement, decision, action).

Errors in testing occur when:

1. A test disagrees with itself-unrepeatable test.
2. One test disagrees with another -- one or both may not be repeatable or may not be valid tests. An invalid test makes a decision based on a parameter not truly related to the decision.
3. Test disagrees with the external validity criterion. This type of error usually remains undetected.

Significant test errors are being made if:

1. A significant percentage of RTOK's exist at any level.
2. High rejection rates exist at any level.
3. The user rejection rate is high.

Test deficiencies should be isolated by conducting a carefully planned experiment under normal production conditions to determine if tests are not repeatable, not valid or not sufficient. Causes of each case and corrective actions are discussed, based on the results of statistical analyses.

The plan requires the following elements: a problem, financial gain resulting from correction, experts, authority, data, a plan and an organized team to conduct the experiment.

CONCLUSIONS: As the devices being tested are becoming extremely accurate compared to most tests and devices, tests

CONCLUSIONS (Continued)

used are only slightly more accurate than the devices being tested. This necessitates the development and revision of tests that will be more and more accurate.

Since conditions at the depot level are often not anticipated by the development engineers, tests must be made efficient by the depot level personnel.

S-24

TITLE: Final Report on Improved Maintenance Procedures for Inertial Guidance Systems.

AUTHOR: Levy, Girard W. et al.

JOURNAL: PRAM Program Office; AFSC, Aeronautical Systems Division; Wright-Patterson AFB, 8 Sept. 1976.

SCOPE: Simulation of the maintenance process to improve testing procedures.

OBJECTIVE: Develop a methodology for locating and optimizing economically significant decisions in the Air Force maintenance process.

SOLUTION APPROACH: Develop an analytical model for simulation of the depot and field maintenance process. Examine alternative tests and test sequencing in terms of system costs and benefits. Total cost divided by the number of missions flown provides a measure of performance for evaluation of alternatives. Apply proposed changes and evaluate. Necessary input data for this simulation will need to be collected.

APPENDICES:

A - Simulation modeling approach.

B - Basic model of maintenance approach.

C - Complex simulation model of the AN/ASN-90 IMU maintenance process

D - Mathematical and decision theory analysis of maintenance decision processes.

E - Discussion of the problem of setting multivariate tolerance limits or thresholds in the testing of complex equipment.

F - Basic data and summaries of the analyses of test repeatability data on a selected portion of the final acceptance test of the AN/ASN-90 IMU.

S-25

TITLE: Operation and Support Cost Characteristics of Testers and Test Subsystems.

AUTHOR: Bogard, D.R. et al.

JOURNAL: RADC-TR-79-334, Final Technical Report, January 1980.

SCOPE: Air Force electronic equipment.

PROBLEM DEFINITION: To investigate and develop guidelines and relationships for use in the development phase of Air Force electronic equipment-program to estimate operation and support (OS) costs associated with various types of testers and test subsystems.

CONSTRAINTS: None.

SOLUTION APPROACH: The cost elements and related parameters affecting support costs are identified. Existing in house and government data on a large number of systems are collected. OS cost parameters are identified. Regression analysis and engineered cost estimates are used to develop OS cost estimated relationships (CER) and guidelines. Knowledge of testers and test subsystems are not required. Details of cost split up and regression analysis technique are discussed. A list of conclusions for testers, test subsystems, software and recommendations are listed separately.

COMPUTATIONAL EXPERIENCE: A computer printout of the multiple linear regression analysis is enclosed for various tester categories.

CONCLUSIONS: Software maintenance costs dominate the cost. Hence it is used as an independent variable, its guideline being the best cost-estimating aid. For test subsystems without software, technical data maintenance cost is highest.

CERs and guidelines, when used early in the development of a weapons system, aid in determining the optimum cost mix of internal testing versus external testing for ground based electronic equipment. Application of CER also helps in predicting 95% confidence interval.

V - REVIEW

V-1 Carroll, B.D. and Smith, E.W., "A Bibliography of Fault Tolerant Computing," AD-739522 (1972).

V-2 "Comparative Analysis of Fault Isolation Procedures," AD-768125 (1973).

V-3 Hakimi, S.L., "Fault Analysis in Digital Systems. A Graph Theoretic Approach."

V-4 Kime, C.R., "Fault-Tolerant Computing: An Introduction and a Perspective," IEEE Transactions on Computers, Vol. C-24 (1975).

V-5 Meyer, J.F. and Rault, J.C., "Fault-Tolerant Computing: An Introduction," IEEE Transactions on Computers, Vol. C-25, (1976).

V-6 O'Reilly, W.T., "A Quantum Step in the State of the Art of M/BIT," Annual Reliability and Maintainability Symposium (1975).

V-7 Pau, L.F., "Diagnosis of Equipment Failure by Pattern Recognition", IEEE Transactions on Reliability, Vol. R-23 (1974).

V-8 Ramamoorthy, C.V., "Fault-Tolerant Computing - An Introduction and an Overview," IEEE Transactions on Computers, Vol. C-20 (1971).

V-9 Reddy, S., "Fault Tolerant Computing - An Introduction", IEEE Transactions on Computers, Vol. C-27 (1978).

V-10 Schertz, D.R., "Fault-Tolerant Computing: An Introduction," IEEE Transactions on Computers, Vol. C-23 (1974).

V-11 Malck, M. and Liu, K., "Graph Theory Models in Fault Diagnosis and Fault Tolerance," Design Automation and Fault-Tolerant Computing, Volume III, Issue 3/4 (1980) Automation.

V-12 Evans, R.A., A Book Review of "Fault Detection and Diagnosis in Chemical and Petrochemical Processes", by David M. Himmelblau (1978).

V-1

TITLE: A BIBLIOGRAPHY OF FAULT TOLERANT COMPUTING.

AUTHOR: Carroll, B.D. and Smith, E.W.

JOURNAL: AD 739522, February, 1972.

PROBLEM DEFINITION: To list all the references in this field.

SUMMARY: Contains a list of 422 articles alphabetically arranged.

Subdivided separately as:

1. Introductions, surveys, and bibliographies.
2. Fault diagnosis of logic network.
3. Analysis and design of digital systems.
4. Validation of computer programs.

Chronological list:

From 1956 - 1971 is given.

V-2

TITLE: COMPARATIVE ANALYSIS OF FAULT ISOLATION PROCEDURES.

JOURNAL: AD 768-125, March 1973.

SCOPE: Any system.

PROBLEM: To discuss applications of four different analytical procedures in fault isolation.

- Half Split Procedure
- Least Square Testing Procedure
- Information Theory Approach
- Probability Approach for Complex Systems and comparison.

HALF SPLIT PROCEDURE: Only one component is failing; for maximum , nearly equal probability of failure of each component/module. Applicable for a series chain like system configuration.

APPROACH: The chain is split into two, and that the half with the fault, is further split to two. The same process is repeated until the fault is pinned down.

LEAST COST TESTING PROCEDURE ASSUMPTIONS: Certain tests must be performed before others - precendence, and a given set of tests must be performed together - proximity.

Cost of test C_i (of ten $_i$) is given

Probability of passing the test for each component (Q_i) is known $(P_i = 1 - Q_i)$. C_i, Q_i & T_i are independent of the sequence of tests.

APPROACH: Minimizes the cost testing sequence. Index $\underline{I_i} = c_i/P_i$ is calculated and the component with smallest $\underline{I_i}$ is tested first and so on - unless overruled by Precedence/Proximity constraints. An example is worked out with eight different components (mechanical, electrical, electronics). Suitable if components are arranged functionally in a series.

INFORMATION THEORY APPROACH: Suitable for multiple failures.

ASSUMPTIONS: Cost of testing at a particular test point, probability of failure of each component are known. Also, cost of applying an external stimulus to a test point is needed.

APPROACH:

Tests are chosen based on a figure of merit.

$$F_i = \frac{\text{amount of information gained from a test}}{\text{Cost of test}}$$

$$F_i = \frac{-P_i \ln P_i - (1-P_i) \ln (1-P_i)}{C_i} ;$$

P_i = Probability that test "i" will pass
F_i is calculated for all possible tests and the test with greatest F_i is conducted first.

A new figure of merit is then calculated using these new costs, and new probabilities. An outline of the procedures is given.
(Only limitations are whether or not the functional descriptions of the system is possible or not). An example is worked out.

PROBABILITY APPROACH FOR COMPLEX SYSTEMS:

Probability of a component failure in a module, for all modules is known. The procedure aims at minimizing the expected amount of time (or cost) penalties paid for a 'testing program' of complex systems. The procedure first determines the failing module and then the failing component within.

The commonly used indices are:

$$A_i = \frac{T_i(1-P_i)}{P_i} ;$$

$$= \frac{T_i}{P_i}$$

$$= \frac{T_i + (1+D_i)\, T_{ri}}{P_i} \text{ (less frequently used)}$$

T_i = Time for testing i^{th} module

P_i = probability that i^{th} module has failed.

D_i = Probability that the test gives i^{th} module as defective given that it is defective

T_{ri} = Time required to search resulting from the tester indicating i^{th} module is good/it is defective.

$$A_{ij} = \frac{T_{ij}}{P_{ij}\,(1-Q_{ij})}$$

Q_{ij} = Probability that no information is gained from the test on the j^{th} component in the i^{th} module.

PROBABILITY APPROACH FOR COMPLEX SYSTEMS (Continued)

In practice, choose either, depending on data availability. Choose lower index first and perform the associated test. Restricted by data available in the system configurations. An index is solved to illustrate the method.

Comparisons of the 4 methods are tabulated.

CONCLUSIONS:

Reasonably complete maintenance record is needed - for all major equipment so that the best possible procedure can be selected, based on these. A background analysis, assumptions, general descriptions of the procedure, are outlined. A literature review of the existing methods is attached. Transfer function method - transfer function changes as the network parameter changes. To provide a quick and easy means of determining a fault isolation procedure, each of the procedures should be developed into a computer program.

V-3

TITLE: FAULT ANALYSIS IN DIGITAL SYSTEMS - A GRAPH THEORETIC APPROACH.

AUTHOR: Hakimi, S.L.

JOURNAL:

SCOPE: Automatic fault diagnosis in ditigal systems, Review.

SUMMARY: This article summarizes all the papers which used a graph-theoretic approach to find the necessary and sufficient conditions for a system to be diagnosable with at most T faults. The system is made up of a number of units. Each unit is assumed to be tested by some other units.

Models which are reviewed here are:

1. Preparata- Metze - Chien Model
2. Hakimi and Amin Model
3. Maheshwari and Hakimi Model
4. Russell - Kime Model

V-4

TITLE: FAULT-TOLERANT COMPUTING: AN INTRODUCTION AND A PERSPECTIVE.

AUTHOR: Kime, C.R.

JOURNAL: IEEE Transactions on Computers, Vol. C-24, No. 5, May, 1975.

SCOPE: Fault diagnosis --- Review.

SUMMARY: Fault-Tolerant computing has been defined as the ability to execute specified algorithms correctly regardless of hardware failures, total system flaws, or program fallacies.
The paper is addressed to the achievement of fault tolerance. Notably, sections are devoted to the fault diagnosis function, to highly reliable systems, to system modeling, and to the system validation function. Each one of these subjects is explained, and all the papers dealing with it are summarized and reviewed.

The last section is devoted to the discussion and analysis of the importance and perspective of large-scale integration (LSI).

V-5

TITLE: FAULT-TOLERANT COMPUTING: AN INTRODUCTION.

AUTHOR: Meyer, J.F. and Rault, J.C.

JOURNAL: IEEE Transactions on Computers, Vol. C-25, No. 6, June 1976.

SCOPE: Fault-Tolerant---Review.

SUMMARY: This paper summarizes, very briefly, papers in the area of Fault-tolerant computing. The first group of papers deal with the subject of fault-tolerant design. The second group of papers considers problems of fault detection and diagnosis in systems composed of interconnected modules. The next group of papers addresses the problem of diagnosing computing systems at module and functional levels. The final group of papers concerns the generation of fault-detection tests for logic networks where the fault class is specified at the logic level.

V-6

TITLE:	A QUANTUM STEP IN THE STATE OF THE ART OF M / BIT.
AUTHOR:	O'Reilly, W.T.
JOURNAL:	Annual Reliability and Maintainability Symposium, 1975.
SCOPE:	Review of BIT

SUMMARY:

This paper discussed the aspect of maintenance of electronic equipment in general. The maintenance is classified into four distinct categories. They are:

1. Check out.
2. Fault Isolation.
3. Remove and replace.
4. Harmonization.

Each category is explained and discussed in detail, then more emphasis has been directed toward the application of the four categories of maintenance in the Airborne Warning and Control System (AWACS) and the Surveillance Radar Functional Group (SRFG) of the AWACS in particular. The effectiveness of AWACS maintenance has been discussed as well as the applicability of Built-in-Test (BIT).

CONCLUSIONS:

The AWACS SRFG Program has achieved specific results with regards to maintainability and in particular the incorporation of built-in-test that serves as a basis for predictions as to future trends and maintenance concepts.

V-7

TITLE: DIAGNOSIS OF EQUIPMENT FAILURES BY PATTERN RECOGNITION

AUTHOR: Pau, L.F.

JOURNAL: IEEE Transactions on Reliability, Vol. R-23, No. 3, August, 1974.

SCOPE: Electromechanical equipment, engines, simple mechanical parts and other non-purely electronic equipments.

PROBLEM DEFINITION: To recognize a failure mode or a set of failures (syndromes) automatically.

ASSUMPTIONS: Total number of different failure causes is small with respect to the total number of equipment observed. The probability distribution of the failure causes has been estimated.

SOLUTION APPROACH: A failure pattern vector is determined using numerical information about the failures, results of nondestructive tests and past history of the system. These patterns are compared with known/learning patterns, stored in a data bank. A compression method of observations about each system, for better discrimination between failure modes and to eliminate redundant tests is discussed. The failure pattern display along with their instances of maintenance control is explained. In accordance with the diagnostic assumptions, rules for sequencing the inspections by the element-by-element method is described. The whole process is divided into learning phase (collecting data), testing phase (processing data) and operational phase (executions of test).

COMPUTATIONAL EXPERIENCE: The data in the example mentioned was processed in an IBM - 370/65. An algorithm for the tests sequence/procedure is mentioned.

CONCLUSIONS: Pattern recognition technique helps make maintenance more efficient. This makes the designer understand the complex relationships between the operating environment, production control and other factors. Success lies on the quality of data records and the reliability of the monitoring sensors used.

V-8

TITLE: FAULT TOLERANT COMPUTING: AN INTRODUCTION AND AN OVERVIEW.

AUTHOR: Ramamoorthy, C.V.

JOURNAL: IEEE Transactions on Computers, Vol. C-20, No. 11, November, 1971.

SCOPE: Computers.

PROBLEM DEFINITION: A study of significant accomplishments in fault detection and location, reliability modeling, analysis and architecture.

SUMMARY: Fault-tolerant computing is defined as "the ability to execute specified algorithms correctly regardless of hardware failures and software errors". The heirarchy of developments of testing procedures is explained briefly. Developments such as (1) partitioning the behavioral characteristics of digital network under known fault modes and using these to develop efficient test patterns, (2) Path sensitizing method as a forerunner to D-algorithm, (3) Boolean difference methods, (4) graph theoretical methods - depending on the structure of the interconnecting subsystems and information flow, and (5) concept of blocking gates.

For multiple faults very little work has been done, though some very promising advances have been made by Bossen and Hong. In any system, the designer's intuition and experience benefit the objectives of the design.

The design and description of the Jet Propulsion Laboratory's STAR computer is provided by its developers, illustrating the ingenious deployment of fault-tolerant principles in the synthesis of an ultra-reliable computer system for space exploration. Software reliability too is emphasized along with a need for much simpler (even if less rigorous) methods to provide partial validations of huge programs.

COMPUTATIONAL EXPERIENCE: None.

CONCLUSIONS: A theory of fault diagnosis is yet to be developed, that could help in designing total test procedures for specific computers under specified cost constraints, considering applications environment, degree of isolations required, cost of developing and testing them.

Microprogramming technique is encouraged. Its impact is highly felt.

V-9

TITLE: FAULT TOLERANT COMPUTING: AN INTRODUCTION

AUTHOR: Reddy, Sudhakar

JOURNAL: IEEE Transactions on Computers, Vol. C-27, No. 6, June 1978.

SUMMARY: Self checking is used to dynamically detect faults.

1. Design of self checkers for m out of n is presented.
2. Computation of roll back distance to achieve a given probability of successful data restoration - in computers with imperfect checking facilities.
3. Relationship between STRONG FAULT SECURE (SFS) logic circuits and totals. Self checking (TSC) networks are studied.
4. Use of binary decision diagrams.
5. Use of random test inputs.
6. Use of Markov Model to describe the behavior of intermittent faults in logic circuits.
7. Test procedures to detect certain functional faults in semi-conductor RAM.
8. A new decoding technique for use with error correcting coding of same basic module.
9. Problem of synchronization in redundant system with multiple copies of a basic module.
10. Performance related reliability measures for computing systems.
11. Models for computing systems with potential hardware/software faults.
12. Digital systems of interconnected units, each unit being capable of completely testing other units.
13. Statistical theory to evaluate the performances of maintenance software in real-time systems.

V-10

TITLE: FAULT-TOLERANT COMPUTING: AN INTRODUCTION.

AUTHOR: Schertz, D.R.

JOURNAL: IEEE Transactions on Computers, Vol. C-23, No. 7, July, 1974.

SCOPE: Fault-Tolerant---Review.

SUMMARY: This problem summarizes, very briefly, all papers in the area of fault-tolerant computing. The first group of papers deals with the design and reliability evaluation of fault tolerant circuits and systems. The other papers deal with the topic of fault diagnosis. The first such group of papers deals directly with the testing of networks, other papers consider the possibility of other fault types in combinational networks. The final paper deals with the design of networks having improved diagnostic properties.

V-11

TITLE: Graph Theory Models in Fault Diagnosis and Fault Tolerance.

AUTHOR: Malck, M. and Liu, K.

JOURNAL: Design Automation and Fault-Tolerant Computing, Volume III, Issue 3/4, 1980.

SCOPE: Review.

SUMMARY: Review graph theory models which are applied in fault diagnosis and fault tolerance and classify the models and their basic features. Starting from the Preparata et al. model in which the system is partitioned into sub-units, test links can be assigned anywhere as needed. Each unit has the capability of testing other units. Following Preparata et al., Barsi et al. improved the model by making it more applicable to real systems. The Maheshwari and Hakimi model takes into account the probabilistic nature of the occurrence of the fault. Fujiwara and Kinoshita fulfilled probabilistically t-fault diagnosability with repair in the Maheshwari and Hakimi model. Mellela and Masson considered the intermittent faults in the Preparata et al. model. Liu and Malck considered fault tolerant capability in Barsi et al. model.

V-12

TITLE: Fault Detection and Diagnosis in Chemical and Petrochemical Processes.

AUTHOR: Himmelblau, David M., 1978.

JOURNAL: Book Reviewed by Ralph A. Evans.

SUMMARY: An introductory book with examples from chemical/ petrochemical processing industries. Deals with reliability and is practically oriented. Discussion of models (PP-90) is excellent. Observed faults and equipment faults are not adequately distinguished.

CONCLUSIONS: Significant limitations of model building must be recognized. They are no more accurate than the physical data which go into them.

X - MISCELLANEOUS

X-1 "A Markovian Approach to Missile Systems Test Sequencing," AD-A050848 (1978).

X-2 Akers, Sheldon B., Jr., "Fault Diagnosis as a Graph Coloring Problem," IEEE Transactions on Computers, Vol. C-23 (1974).

X-3 Biegel, J.E., "A Multilevel Modularization Technique Designed to Minimize Life Cycle Costs for Large Systems", AIIE Proceedings - 1979 Spring Annual Conferences.

X-4 Chang, H.Y., "A Distinguishability Criterion for Selecting Efficient Diagnostic Tests," Spring Joint Computer Conference (1968).

X-5 Puri, N.N., "Fault Isolation Via State Variable Analysis," AD 733-817 (1974).

X-6 Ramamoorthy, C.V. and Mayeda, W., "Computer Diagnosis Using the Blocking Gate Approach," IEEE Transactions on Computers, Vol. C-20 (1971).

X-7 Rosenthal, A., "Decomposition Methods for Fault Tree Analysis," IEEE Transactions of Reliability, Vol. R-29 (1980).

X-8 Nakagawa, T., "Replacement Policies for a Unit with Random and Wearout Failures", IEEE Transactions of Reliability, Vol. R-29 (1980).

X-9 Swets, J.A. et al., "Assessment of Diagnostic Technologies," Science, Vol. 205, No. 4407 (1979).

X-10 Susskind, A.K. "Diagnostics for Logic Networks", IEEE Spectrum (1973).

X-11 Spray, G.W. et al., "A Model of Maintenance Decision Errors," 1982 Proceedings Annual Reliability and Maintainability Symposium.

X-12 Liguori, Fred, "Introduction to Current Computer Aids to Digital Test Design for Automated Test Equipment", SETE Workshop Proceedings (1974).

X-13 Genet, R.M., and Billig, P.L., "Statistical and Cost Effectiveness Analysis of Acceptance Specifications and Initial Tests for Gyroscope Float Assemblies", Report No. 69-4, Aerospace Guidance and Metrology Center Newark Air Force Station, Newark, Ohio 43055 (1969).

X-14 Abraham, J.A. and Thatte, S.M., "Fault Coverage of Test Programs For a Microprocessor," 1979 IEEE Test Conference, Cherry Hill, New Jersey.

X-15 Hartwell, W.T. et al., "A Fault Tolerant Memory for Duplex Systems," IEEE Transactions on Reliability, Vol. R-27 (1973).

X-16 Nakagawa, T., "Mean Time to Failure With Preventive Maintenance," IEEE Transactions of Reliability, Vol. R-29 (1980).

X-17 Pieper, W.J. and Pinkus, A.L. "Computer Generated Trouble Shooting Trees - The Program," AD-785 139 (1974).

X-18 Freedy, A., and Lucaccini, L.F., "Adaptive Computer Training System (ACTS) For Fault Diagnosis in Maintenance Tasks," Human Detection and Diagnosis of System Failures (1980).

X-19 Lihou, D.A., "Aiding Process Plant Operators in Fault Finding and Corrective Action", Human Detection and Diagnosis of System Failures, (1980).

X-20 Genet, R.M., "The Application of Stepwise Linear Regression Analysis, Discriminant Analysis, and Chi Square Analysis to Gyroscope Float Group Prediction", Interim Report Number 69-16, Aerospace Guidance and Metrology Center, Newark Air Force Station, Newark, Ohio.

X-1

TITLE: A MARKOVIAN APPROACH TO MISSILE SYSTEMS TEST SEQUENCING.

AUTHOR: AD A050848

JOURNAL: April, 1978.

SCOPE: Missile systems, systems with limited testing resources.

PROBLEM: Given a new missile system, a set of required capabilities, and a limited set of testing resources, to verify accomplishments and non accomplishments as efficiently as possible with highest expected reward decision criteria.

ASSUMPTIONS/
CONSTRAINTS: Markovian assumption; probability of transitioning from state to state is solely dependent on the state presently occupied.

SOLUTION APPROACH: Defines success as meeting the objectives of the test. Chooses tough tests with lower probability of success, but higher pay-offs. A four state test diagram is described, in which the next state depends on the success or failure of the present test. Using this, a transaction matrix is tabulated (probability P_i) from which the rewards of a test are computed. Other parameters such as

i) $\emptyset_{ij}$ (n) = probability of being in state j, after n transitions, and starting from state i.

ii) $V_{ij}(n)$ = number of times test state j is occupied through n transitions given that the process started in i, calculated using $\emptyset$ Mx. Then expected reward (R) Mx is calculated. An example to illustrate the abstract concepts is given - considers a ZAP missile starting with four factors and two conditions, he goes one step ahead including various costs and more conditions.

A 3-dimensional sensitivity has been conducted in the sense that i) costs and benefits ii) probabilities iii) decision criteria are all considered. Appendix contains various tabulations and transitions diagrams.

COMPUTATIONAL EXPERIENCE: None.

CONCLUSIONS: Model assists the designer in his choice of critical starting point in test sequence, based on Markovian assumption as well as the ability to (1) identify discrete test states (2) enumerate costs and benefits

CONCLUSIONS (Continued)

and (3) determine rules and a priori probability for programming from test state to test state.

X-2

TITLE: FAULT DIAGNOSIS AS A GRAPH COLORING PROBLEM

AUTHOR: Akers, Sheldon B., Jr.

JOURNAL: IEEE Transactions on Computers, Vol. C-23, No. 7, July, 1974.

SCOPE: Directed, acyclic graphs or circuits with fanout free configurations.

PROBLEM DEFINITION: To rephrase the problem of fault finding as a graph coloring labeling problem and to mention a few well known concepts in graph labeling and to give a procedure to test, by a node coloring procedure.

CONSTRAINTS: The circuit must be a fanout free network, i.e., for directed, acyclic graphs only.

SOLUTION PROCEDURE: Any given logic network/graph is converted into a "directed acyclic" graph. A "test" is defined as a labeling of each node with either a 0 or 1 such that (1) no 1-nodes are adjacent (2) every fanout has at least 1-node. Such a scheme yields a proper labeling or proper coloring. So every coloring has to satisfy the above two properties. Graphs which are of at least two colors are bipartite graphs.

A fanout free network with every gate having one output only and every primary input driving only one gate comes under a class of networks which can be grouped under bipartite. This permits a 2-colouring. A set of 5 tests is considered as an example and the various questions commonly faced are answered. From this set of 5 tests, tests which are not necessary are suitably eliminated. A detailed procedure for such elimination is presented. Sufficient examples are considered at crucial points. Basically a graph theory approach is used.

The labeling procedure for a fanout free network is summarized.

CONCLUSIONS: If a network can be written as fanout free, then the graph coloring procedure is a suitable method to analyze it.

Most of the fault diagnosis problems are amenable to a graph coloring procedure. The concepts of dominating set and independent set are not considered in this paper.

X-3

TITLE: A MULTILEVEL MODULARIZATION TECHNIQUE DESIGNED TO MINIMIZE LIFE CYCLE COSTS FOR LARGE SYSTEMS.

AUTHOR: Biegel, J.E.

JOURNAL: AIIE Proceedings - 1979 Spring Annual Conference

SCOPE: Modularization of Systems.

PROBLEM DEFINITION: Studying the multilevel modularization of large systems. A system is first decomposed into functional elements then reconstructed into modules, each module containing one or more functional elements. The modules are then collected into subassemblies. The subassemblies into higher level subassemblies, etc. The criteria is to form the collected sets in such a way that the life cycle cost is minimum.

ASSUMPTIONS: The function of the component and its functional relationship with its neighbors in a module are irrelevant.

SOLUTION APPROACH: The problem is in general a nonlinear, integer programming problem. It is solved here using a heuristic approach.

COMPUTATIONAL EXPERIENCE: The procedure is coded in Fortran and has been used to solve a trial problem of 100 elements and been shown to work acceptably, although it has not been proved to be an optimal solution method.

CONCLUSIONS: A computer routine that has been developed to perform the modularization is explained. The routine is a generalized one such that it can do any number of levels of modularization without alteration of the algorithm. Also, the solution is independent of the function of the element and depends only upon the constraints imposed.

X-4

TITLE: A DISTINGUISHABILITY CRITERION FOR SELECTING EFFICIENT DIAGNOSTIC TESTS.

AUTHOR: Chang, H.Y.

JOURNAL: Spring Joint Computer Conference, 1968.

SCOPE: Digital circuits - electronic telephone switching systems, air-borne computers, etc.

PROBLEM: To compute the figure of merit of tests to derive efficient testing procedures using the DISTINGUISHABILITY criterion.

SOLUTION APPROACH: Two other criteria - The partition method and information gain criteria are briefly described. A test to distinguish each faulty machine is needed. This leads to $\frac{N(N+1)}{2}$ machines to be distinguished. A method to calculate the distinguishability is given. Applications of the distinguishability criterion to derive an efficient testing procedure is illustrated by an example - with 10 faults to be identified to 3 modules. A procedure is given for distinguishing faults to (i) component level (ii) module level.

COMPUTATIONAL EXPERIENCE: None.

CONCLUSIONS: Identifies failures only to the circuit package/ smallest replaceable module level. By adapting to isolate to the module level, the program memory required to store the diagnostic testing procedure is significantly reduced.

This criterion is compatible with the concept of information gain developed by Johnson et al. for component level diagnosis. For module level replacement, the sequential testing procedure based on distinguishability criterion yields shorter sequences with better resolvability.

X-5

TITLE: FAULT ISOLATION VIA STATE VARIABLE ANALYSIS

AUTHOR: Puri, N.N.

JOURNAL: AD 773-817, Jan. 1974.

SCOPE: Linear Systems.

PROBLEM DEFINITION: To develop an algorithm for the parameter identification of a circuit from its frequency response.

ASSUMPTIONS: None of the circuits contain nonlinear devices or devices operating in their non-linear region. The system is observable.

APPROACH: Contains an algorithm for the parameter identification of a circuit from its frequency response. A new technique is used to find the element values of the components of a circuit under test using Fast Fourier Transforms-directly and accurately. This technique uses a computer program from the wiring diagram of the circuit.

State variable formulation of the network based on topological configurations made using computer programs.

Formulations of a conjugate gradient algorithm involving the state variable model to obtain the matching values of the entries in the various matrices of the state variable model and hence the isolation of the faulty element is explained.
The state equation $\underline{X} = \underline{F}\,\underline{X} + \underline{G}\,\underline{U}$; $\underline{Y} = \underline{H}^T\,\underline{X} + \underline{C}\,\underline{U}$ is defined and obtained by choosing a suitable tree and writing its cutset, tieset equation. From these state equations the observation vector (o/p) is calculated.

Next, to obtain the element of the state matrices, by frequency response methods, a fault isolation algorithm (J) is given involving a vector P (of the components of the network) from which $\frac{J}{P_i}$ is calculated.

CONCLUSIONS: The algorithm is summarized. The iteration is stopped when gradient is near zero. From this gradient, a matching value of the entries in the various matrices of the state variable model is obtained. This is made use of in isolating faulty elements.

This is a mathematical paper. Just by getting the state variable model, how a fault can be isolated is not clearly explained.

X-6

TITLE: COMPUTER DIAGNOSIS USING THE BLOCKING GATE APPROACH.

AUTHOR: Ramamoorthy, C.V., and Mayeda, W.

JOURNAL: IEEE Transactions on Computers, Vol. C-20, No. 11, November 1971.

SCOPE: An alternative technique to computer system diagnosis (as opposed to fault test point methods) is dealt with.

PROBLEM DEFINITION: To decide the maximum distinguishability (fault isolation) of a system, based on a graph theory approach using blocking gate methods rather than the test points method.

CONSTRAINTS: Faults are assumed to be permanent until repaired, i.e., not intermittent faults. Also the probability of a set of concurrent faults occuring and nullifying their efforts mutually is very small.

COMPUTATIONAL EXPERIENCE: An algorithm to determine the optimal location of blocking gates for maximum distinguishability of faults under arbitrary cost constraints is constructed.

APPROACH: A 'Blocking Gate' is defined. Test signals are inserted at the specified inputs and results monitored at the primary o/p points. A signal flow graph approach is followed. Its advantages are mentioned. When a gate is blocked, it prevents onward transmission of the responses of any fault reaching it. A handful of lemmas and theorems are mentioned on graph theory. A couple of examples are given. The blocking gate method, conceptually simple, varies in complexity to implement. A complex system is represented by graphs and subsequent analysis based on graph theory is made use of in system diagnosis. A structural representation of the system is made and then a set of blocking gates can be inserted at strategic sites in the system.

CONCLUSIONS: No implementation technique is considered in depth, but elementary principles of this method are given. Using the algorithm, a nearly minimum set of test gates for maximum distinguishability is obtained.

The blocking gate method, when used in conjunction with the test points method yields a near optimal test set. A distinct relationship appears between path sensitizing method, Roth's D-Alg, and this blocking gate approach.

X-7

TITLE: Decomposition Methods for Fault Tree Analysis.

AUTHOR: Rosenthal, A.

JOURNAL: IEEE Transactions of Reliability, Vol. R-29, No. 2, June 1980.

SCOPE: FAULT tree analysis.

PROBLEM DEFINITION: Exploring the idea of "Modularization" and its effect in solving the problems of the exponential size of fault trees when it grows, and formulating the problem of finding all modules of a fault tree as an extension of the problem of finding all cut points of an undirected graph.

ASSUMPTIONS: A module of a fault tree is a set of at least two events which has only one output to the rest of the tree and no inputs from the rest of the tree.

SOLUTION APPROACH: Graph theory.

COMPUTATIONAL RESULTS: The suggested procedure is ceded to FORTRAN and the program is available as a supplement.

CONCLUSIONS: A procedure and a ceded FORTRAN program is suggested to find modules of a 1000-event fault tree in a fraction of a second. Also a generalized module is defined.

X-8

TITLE: Replacement Policies for a Unit with Random and Wearout Failures.

AUTHOR: Nakagawa, T.

JOURNAL: IEEE Transactions of Reliability, Vol. R-29, No. 4, Oct. 80.

SCOPE: Miscellaneous.

PROBLEM DEFINITION: An operating unit enters a wearout failure period (period II) at a fixed time, after it has operated continuously in a constant hazard rate period (period I). Consider replacement models of the following three cases: a) the unit is replaced at failure, b) the unit undergoes minimal repair at failure, c) the unit is replaced at failure only in a wearout failure period.

ASSUMPTIONS:

1. The unit enters period II after it has operated in period I.
2. The failure time of the unit in period II is independent of that in period I.
3. The hazard rate is continuous and monotonely increasing.
4. The failed unit is detected as soon as it fails.
5. The times for repair or replacement are negligible.

SOLUTION APPROACH: Probabilistic approach.

COMPUTATIONAL EXPERIENCE: None.

CONCLUSIONS: Optimum replacement policies which minimize the s-expected cost rate for each model are presented.

X-9

TITLE: Assessment of Diagnostic Technologies.

AUTHOR: Swets, John A. et al.

JOURNAL: Science, Vol. 205, No. 4407, Aug. 1979.

SCOPE: Evaluation of diagnostic systems using relative operating characteristic analysis.

PROBLEM DEFINITION: The current methods of comparing diagnostic systems are inadequate because they fail to accurately model the decision process. The method presented claims to have overcome these shortfalls.

SOLUTION APPROACH: Two radiologic techniques - computed tomography and radionuclide scanning are to be compared. The procedure utilizes real cases and real diagnostic tasks where verification of the presence or absence of a brain tumor has been verified by autopsy or by survival with no symptoms for 8 months. Following a statistically controlled study the results are compared using relative operating characteristic (ROC) analysis (from the general theory of signal detection).

The ROC is a curve showing the various trade-offs existing between proportions of true-positive and false-positive responses, as the decision criterion is systematically varied, for a given capacity to discriminate between positive and negative cases.

CONCLUSIONS: The ROC may form the basis for an evaluation of the usefulness of a diagnosis system. The ROC is a means of determining the response probabilities appropriate to the best available estimates of the values, costs, and event probabilities that inhere in the relevant diagnostic and therapeutic context.

X-10

TITLE: Diagnostics for Logic Networks

AUTHOR: Susskind, A.K.

JOURNAL: SETE Workshop Proceedings (Feb. 74)/IEEE Spectrum (October 73).

SCOPE: Design of diagnostic tests for modest size networks.

PROBLEM DEFINITION: The lack of test points in LSI circuits, the need for efficient test procedures, and increased need for complete testing of electronic equipment, have increased the interest in techniques for detecting and locating failures in complex digital networks.

CONSTRAINTS: The techniques covered are economically feasible only for networks of modest size (hundreds of gates). The balance of the article deals with structure tests which are lengthy though complete as opposed to function tests which are feasible for large systems but are usually not complete.

SUMMARY: The most universally accepted fault model is the stuck-at (SA) model. Tests based on this model deal with static faults. It is not clear how well the SA model fits LSI. Faults such a shorting between adjacent conducting lines and intermittent faults are not covered by the SA model. The problem of multiple faults can't be ruled out in the case of production testing and care should be taken not to misinterpret results.

Fault insertion and simulation may be used to appraise the effectiveness of test procedures. Fault insertion has the advantage of complete fidelity when the equipment is available. When it is not, such as in the design stage, simulation may be economically feasible.

For combinational logic two techniques, path sensitization using Boolean difference and the D algorithm method, are given and provide tests based on the SA model. For the problem of multiple faults an overview of the SPOOF algorithm is given.

For sequential networks the three major ways of finding tests are (1) by verifying functional characteristics, (2) by translating the network into the related iterative circuit, and (3) by verifying the state-table for the given network. Only the first two have gained practical acceptance.

The fundamental cause for the difficulty in finding tests for sequential circuits is the fact that the

SUMMARY (Continued)

state variables are not available for inspection when a sequential network is tested. Much can be done to improve this in the areas of design and layout.

CONCLUSIONS: Progress still needs to be made in the areas of intermittent faults and fault models for LSI technologies. Also diagnostic considerations need to be incorporated into design rules in the future.

X-11

TITLE: A Model of Maintenance Decision Errors

AUTHOR: Spray, G.W. , Teplitz, C.S., Herner, A.E. and Genet, R.M.

JOURNAL: 1982 Proceedings of the Annual Reliability and Maintainability Symposium

SCOPE: Decision errors within equipment

PROBLEM DEFINITION: Decision errors within equipment repair processes can seriously impact the cost and quality of maintenance. This paper discusses some of the causes of these errors.

ASSUMPTIONS: All noise sources are set to zero and the only variation is the time to failure.

COMPUTATIONAL EXPERIENCE: 1000 random sample of failure times are studied.

CONCLUSIONS:

1. A simulation model is discussed which includes a highly-simplified maintenance process with a source of decision errors.
2. Several logic hypotheses regarding decision errors in maintenance are then suggested.
3. A model is used to evaluate these hypotheses.

X-12

TITLE: Introduction to Current Computer Aids to Digital Test Design for Automated Test Equipment

AUTHOR: Liguori, Fred

JOURNAL: SETE Workshop Proceedings (Feb. 74)

SCOPE: Digital simulation for circuit design and testing

PROBLEM DEFINITION: Micro-miniaturization has made digital devices easy to model but has also drastically increased the amount of tests required for each module. This has made computer simulation practical as well as necessary in many cases. So it is essential for ATE test designers and systems engineers to understand the new software tools available. Some of the more successful current systems for computer aided test design are presented.

ASSUMPTIONS: A review of testing techniques and terminology is presented including types of static and dynamic testing. Testing requirements are determined by the nature of the circuit and the purpose of the test (design, production, or maintenance testing). This paper deals primarily with maintenance testing, so the nature of the circuit and its failure modes are of concern. Most digital circuits are combinatorial logic circuits so the paper deals with these. For combinatorial logic static testing is adequate if the design was good and avoided degradation effects. Digital testing inherently requires a large number of test patterns to test all circuit functions. If the test patterns and test programs are automatically generated by computer then very accurate fault detection and isolation can be achieved in very short periods of time.

SOLUTION APPROACH: Combinatorial logic is easy to model. The approach to digital simulation is to build up a library of basic element characteristics in the simulation model. These elements are then copied and linked into the model of the system to be simulated. This simulation technique forms the basis of all effective computer aided circuit design and testing systems.

EXAMPLES: Discussed are the design, applications and limitations of the following Computer Aided Test Design Systems:

1) LASAR II (Logic Automated Stimulus and Response) - LTV Corp.
2) FAIRSIM II/FAIRGEN - Fairchild
3) TESTAID - Telpar Inc.
4) COMTEST/TESTGEN - Westinghouse
5) FLASH (Fault Logic and Simulation Hybrid) - Micro Inc.

EXAMPLES (Continued)

6) TGEN - RCA
7) FAULTS II (Fault Analysis Using Logical Test Sequencing) - General Dynamics
8) SALT (Sequential Automated Logic Test System) - IBM
9) TASC (Terminal Access Simulation and Computation System) - Pacific Applied Systems Inc.

X-13

TITLE Statistical and Cost/Effectiveness Analysis of Acceptance Specifications and Initial Tests for Gyroscope Float Assemblies

AUTHOR: Genet, R.M. and Billig, P.L.

JOURNAL: Report No. 69-4, Aerospace Guidance and Meterology Center Newark Air Force Station, Newark, Ohio 43055

PROBLEM DEFINITION: To determine what changes, if any, should be made to the present Motor and Float (part of the G-200 Gyroscope, a component in the LN-12 Inertial system) specifications. Mainly, to determine if a motor current variation specification should be added to the present specification, and to determine what other changes in the present specification might reduce the present failure rate of the Motor Float Assemblies. Therefore the report discusses the specification and testing of the Motor and Float as well as the cost/effectiveness tradeoff.

SOLUTION APPROACH: Statistical Analysis

COMPUTATIONAL EXPERIENCE: Regression analysis was applied using a "composite score" based on the different test scores which were computed by forming a composite group of data from "good" groups and "bad" ones with the same ratio of good to bad as actually existed of the Motor and Float (3 to 1). With this ratio in mind, the first 27 (of 30) of the good floats and the 9 bad floats were selected to form the composite group of floats. Next, a score of 100 was assigned to each of the good floats and a score of 0.0 to each of the bad floats. Accordingly, the averages and standard deviations for all parameters were computed. The correlations between the variables and the good/bad score were then computed and the intercorrelations between the variables were computed. Next, multiple linear regression analysis was used to determine the coefficient that would best predict the score value. The actual parameter values for each of the 36 wheels were used to calculate the score values. A fail/pass point was then chosen and a "Box Score" formed.

CONCLUSIONS:

1. Recommended changes in the present parameter's specifications are presented and discussed.
2. It is recommended to use the composite score instead of individual tests.
3. Multiple regression analysis could only serve as a non-optimal method of determining a composite score. The use of a multivariate analysis technique is required if optimum results are derived, i.e. the composite score approach is the

CONCLUSIONS (Continued)

preferred approach, and an optimum composite scoring technique can be established through the use of multivariate analysis and better data.

X-14

TITLE: FAULT COVERAGE OF TEST PROGRAMS FOR A MICROPROCESSOR

AUTHOR: Abraham, J.A. and Thatte, S.M.

JOURNAL: 1979 IEEE Test Conference

SCOPE: Microprocessors - Design and Testing

PROBLEM DEFINITION: To quantify the fault coverage of tests by simulation at logic level with single s-a-o or s-a-l faults.

SUMMARY: Classical methods of testing digital logic starting at the gate levels have been known to be prohibitively complex. Functional tests for microprocessors are based on testing them for all instructions for some set of operands. Such an attempt is definitely not a complete one.

A fault model describing various functional primitives, allow one to describe faulty behavior without getting into the details of the microprocessor. Such fault models are described. Instead of finding a pattern to detect each fault, the faults detected by a test pattern is considered. A TESTAID III fault simulator from Hewlett-Packard was used for this purpose.

RESULTS ANu CONCLUSIONS: 90% of all the faults were detected. This basic approach can be used to derive comprehensive tests for any microprocessors. This can be generalized to include a complete system, not just the chip.

X-15

TITLE: A Fault Tolerant Memory for Duplex Systems

AUTHOR: Hartwell, W.T. et al.

JOURNAL: IEEE Transactions on Reliability, Vol. R-27, No. 2, June, 1978

SCOPE: Memory Systems - Duplex and Simplex

PROBLEM DEFINITION: To design fault tolerant memory systems to permit automatic repair of multiple faults without loss of error detection.

ASSUMPTIONS: None

SOLUTION APPROACH: Makes use of bit swapping to achieve high system availability with minimum redundance. Details of swapping principle and implementation are explained. At any instant of time, only one unit will be ON-LINE and the other is OFF-LINE. On detection of an error, swapping occurs, representing a typical electronic switching system. If the error is non-correctable, the machine is marked defective and is a case of manual repair. The module size is kept as low as 4K to reduce swapping costs.

COMPUTATIONAL EXPERIENCE: None.

CONCLUSIONS: This method chosen for swapping depends basically on the device failure rate,memory size, error-corrections costs, maintenance costs and reliability requirements.

X-16

TITLE: Mean Time to Failure With Preventive Maintenance

AUTHOR: Nakagawa, T.

JOURNAL: IEEE Transactions of Reliability, Vol. R-29, No. 4, Oct. 1980

SCOPE: Electronic Systems

PROBLEM DEFINITION: To calculate the mean time to failure with imperfect prevention maintenance (PM) and the S-expected number of PM before failure

ASSUMPTIONS: PM is done at times kT and the system becomes X-units of time younger at each PM. PM time is negligible. After every PM, component failure rate is same as before, but the components are as good as new with a different probability.

COMPUTATIONAL EXPERIENCE: None

RESULTS AND CONCLUSIONS: Final results of the analysis are mentioned and are proved as a supplement.

X-17

TITLE: Computer Generated Troubleshooting Trees — The Program

AUTHOR: Pieper, W.J. and Pinkus, A.L.

JOURNAL: July 1974, AD-785 139

SCOPE: Electronic Systems

PROBLEM DEFINITION: To develop, use and try out a computer program to prepare troubleshooting trees by computer.

ASSUMPTIONS: None

SOLUTION APPROACH: A Fortran IV approach. It inputs information on system data flow, component reliability and costs of available tests. The most efficient sequence of tests to isolate all faults is arrived at, iteratively, based on information gains of each test. After each test, IGUC is recomputed and the process repeated. An example of a 300 component electronic system is analyzed. Program listing is included.

COMPUTATIONAL EXPERIENCE: Fortran IV

RESULTS AND CONCLUSIONS: 100% isolation is not achieved. Significant refinements to the technology are suggested to make it operational.

X-18

TITLE: Adaptive Computer Training System (ACTS) For Fault Diagnosis in Maintenance Tasks

AUTHOR: Amos Freedy and Luigi F. Lucaccini (Perceptronics, Inc.)

BOOK: Human Detection and Diagnosis of System Failure, 1980

SCOPE: Training Using Adaptive Computer Aided Instruction.

OBJECTIVE: The ACTS focuses on improving and sharpening higher-order cognitive skills in electronics troubleshooting.

SOLUTION APPROACH: ACTS incorporates an adaptive computer program which learns the student's diagnostic and decision value structure, compares this to that of an expert, and adapts the instructional sequence so as to eliminate discrepancies. An expected utility or multi-attribute utility model is the basis of the student and instructor models which, together with a task simulator, form the core of ACTS. The student model is dynamically adjusted using a trainable network technique of pattern classification. The training content and problem presentation sequence are generated with heuristic algorithms. ACTS is implemented on an Interdata Model 70 minicomputer and uses interactive graphics terminals.

STUDY RESULTS: A preliminary study was performed with two groups of six subjects each. One group was trained with ACTS the other using the actual circuits. The results were extremely promising. It is anticipated that in the near future studies will be undertaken in the operational training environment.

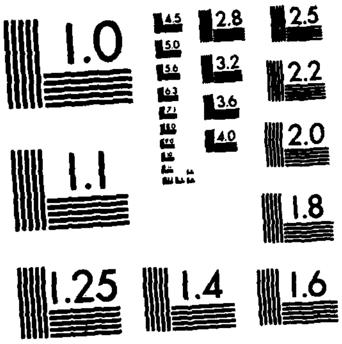
AD-A126 167 ANALYTICAL PROCEDURES FOR TESTABILITY(U) OKLAHOMA UNIV NORMAN SCHOOL OF INDUSTRIAL ENGINEERING A A ALY ET AL. JAN 83 RADC-TR-83-4 F30602-81-C-0012 4/4

UNCLASSIFIED F/G 14/2 NL

END

FILMED

DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

X-19

TITLE: **Aiding Process Plant Operators in Fault Finding and Corrective Action**

AUTHOR: David A. Lihou

JOURNAL: Human Detection and Diagnosis of System Failures, 1980

SCOPE: Fault finding by interaction with a computer using fault symptom matrices.

PROBLEM DEFINITION: Fault finding relies on the correct interpretation of a set of deviations in measured process variables, which relates to single or multiple faulty state. The process variables and locations of the plant form a two dimensional matrix. The elements of the matrix are the symptoms which process variables are expected to display, in response to a specific cause.

SOLUTION APPROACH: Fault Symptom Matrices are stored in a computer as a Fault Symptom Equation. The operator can then ask the computer to identify the fault given the State Matrix at the time. The computer may also be asked to advise the operator on the appropriate corrective action.

CASE STUDY: The method was implemented on a computer for the recovery of acetone. Using an operability study the fault symptom equations were entered into the computer. Even probabilities based on the Weibull distribution were calculated. Then the optimal checking sequence was found by first checking equipment with the lowest checking time/probability.

CONCLUSION: Based on the results it was found to be beneficial to install new gages and arrange for preventive maintenance to avoid not being able to prevent hazardous events.

X-20

TITLE: The Application of Stepwise Linear Regression Analysis, Discriminant Analysis, and Chi Square Analysis to Gyroscope Float Group Prediction

AUTHOR: Genet, R.M.

JOURNAL: Interim Report Number 69-16, Aerospace Guidance and Meteorology Center, Newark Air Force Station, Newark, Ohio

PROBLEM DEFINITION: The analysis of the G-200 gyroscope repair process at AGMC, specially the analysis of a float screening test for G-200 gyroscopes suspected of needing repair. The gyroscope considered consists of a motor, rotating mass, two bearings, and a spherical shell. These parts taken together are referred to as the "float". A test was devised to evaluate float performance based on the composite of several float tests. This test and its score was named "Composite Score Test". This report analyzes data gathered on ten float parameters measured during the normal application of the "Composite Score Test". Primary emphasis was given to trying to predict whether a gyroscope would "fail diagnostic drift with a disposition of replace float" or "pass all tests at AGMC and be shipped to the customer" if it was known in advance that one of these two actions was sure to happen.

COMPUTATIONAL EXPERIENCE: Data from 600 gyroscopes was used. The status of these 600 units was divided into 14 different groups. The best prediction was made based on the ten measured float parameters, whether gyroscopes would subsequently fail diagnostic drift, or leave AGMC as "good" units. Group 1 (failed Diagnostic Drift) and Group 7 (sold to field) were then selected for detailed analysis. Using 86 items from Group 1 and 152 items from Group 7. Each group has been divided into two even subgroups with the first halves of the groups called the "set-up data" and the second halves the "calibration data". Ten paramters have been measured on each item. Given only the set up data from 43 items from Group 1 and 76 items from Group 7, a prediction formula that will be likely to determine group membership with calibration data is found using a stepwise Linear Regression Analysis Procedure developed at UCLA after assigning two different arbitrary values to the dependent variables depending on which group the item belong to. The values of the arbitrary values and the ten measured float parameters served as the data input for the regression analysis.

Also two BMD biomedical computer programs in the area of Discriminant Analysis were run.

COMPUTATIONAL EXPERIENCE (Continued)

A quick (and dirty) chi square analysis was also performed.

A comparison of the results of different methods was presented.

MISSION
of
Rome Air Development Center

RADC plans and executes research, development, test and selected acquisition programs in support of Command, Control Communications and Intelligence (C^3I) activities. Technical and engineering support within areas of technical competence is provided to ESD Program Offices (POs) and other ESD elements. The principal technical mission areas are communications, electromagnetic guidance and control, surveillance of ground and aerospace objects, intelligence data collection and handling, information system technology, ionospheric propagation, solid state sciences, microwave physics and electronic reliability, maintainability and compatibility.

END

FILMED

4-83

DTIC